2026 IT Confidence Index

Q3: PROTECT

A Strategic Briefing for Business and Compliance Leaders

ISOutsource®
Where IT Means Business

CEO Foreword: Naveen Rajkumar – CEO, ISOutsource

In previous editions of the IT Confidence Index, we focused on visibility and efficiency – the need for leaders to see their environments clearly and ensure their investments deliver business value. But clarity and efficiency alone are not enough.

The realities organizations face today are different.

Every business operates in an environment where disruption is not hypothetical. It is expected. Cyberattacks no longer target only large enterprises. Operational failures no longer happen in isolation. The window between identifying a vulnerability and exploiting it has narrowed to minutes and hours, not weeks and months.

Protection, in this context, is not a security function. It is a business requirement. It is the ability to continue business operations when systems fail, recover data after it has been compromised, and the ability for leadership to make decisions with full visibility into risk.

Across client environments, one pattern is clear: organizations experiencing the most disruption are not the ones lacking tools. They are the ones that lack preparedness, validation, and governance.

This quarter, we focus on what it means to operate with resilience.

Protection is not about avoiding every incident. That is not realistic. It is about ensuring that when disruption occurs, the business continues to operate, recover, and move forward without lasting damage.

The organizations that understand this shift are not just more secure.
They are more resilient, more responsive, and ultimately more competitive.

Naveen Rajkumar
CEO, ISOutsource

PROTECT

Protection is often misunderstood as a cybersecurity initiative. In practice, it is broader and more consequential.

It is the system of controls, processes, and decisions that ensures a business can continue operating in the face of disruption.

Across client environments, a consistent pattern emerges. Organizations believe they are protected because controls exist. Backups run. Security tools are installed. Policies are documented. But when those environments are tested under real conditions, the gaps become visible: recovery plans that exist but have never been executed, security controls that are implemented but not validated, risks that are known but not actively managed, and leadership teams that lack visibility into operational exposure.

Protection fails not because nothing is in place, but because what is in place has not been tested, governed, or aligned to business outcomes.

The organizations that operate with confidence are not the ones that have avoided disruption. They are the ones prepared for it.

THIS INDEX EXAMINES PROTECTION ACROSS FOUR DIMENSIONS:

1. **PROTECT OPERATIONS**
   Resilience is defined by the ability to recover quickly and operate through disruption. Without tested recovery strategies and resilient infrastructure, downtime becomes inevitable.

2. **PROTECT DATA & SYSTEMS**
   Security controls only reduce risk when they are actively managed, validated, and aligned to current threats. Unmanaged environments accumulate hidden exposure over time.

3. **PROTECT STRATEGIC DECISION-MAKING**
   Leadership cannot manage what it cannot see. Without governance, visibility, and alignment, IT risk becomes a blind spot in business strategy.

4. **PREPARING FOR AI RESPONSIBLY**
   AI adoption introduces new layers of operational and security risk. Without governance, organizations accelerate exposure faster than they realize.

DIMENSION 1: PROTECT OPERATIONS

Resilience is Measured at the Point of Failure

Most organizations evaluate their IT environment based on their daily performance. Systems are running. Users are productive. Issues are resolved as they arise. This creates a false signal of stability.

The true test of an IT environment does not occur during normal operations. It occurs at the moment of disruption.

- A critical server fails.
- A ransomware attack locks systems.
- A cloud service outage disrupts access.

At that point, the question is no longer whether systems work. It is whether the business can recover.

Across client environments, one of the most consistent gaps is not the absence of recovery plans. It is the assumption that those plans will work when needed. In practice, recovery often fails for reasons that are predictable: backup systems have not been tested in real scenarios, recovery dependencies are undocumented, restoration timelines are underestimated, critical applications are not prioritized correctly, and infrastructure contains single points of failure.

These gaps do not appear during normal operations. They become visible only under pressure.

KEY SIGNAL

Recovery is tested, documented, and aligned to business priorities.

LEADERSHIP QUESTION

If your most critical system failed right now, does your organization know exactly how to recover it, how long it would take, and what operations would look like during that time?

Case in Point

A Seattle-based nonprofit experienced a ransomware attack that resulted in a complete loss of access to its IT environment.

Hackers demanded $200,000 in cryptocurrency and threatened to delete all data if payment was not made. When ISOutsource teams arrived, they identified a critical issue: there was no disaster recovery plan and no reliable backup strategy in place. The organization ultimately restored from a backup that was one year old, resulting in total loss of operational systems, over a year of data loss, and significant disruption to organizational operations. This was not a failure of security tools alone. It was a failure of operational resilience.

Recovery is tested, documented, and aligned to business priorities.
In resilient environments:

- Recovery plans are tested on a defined cadence.
- Backup systems are validated, not assumed.
- Critical systems are mapped and prioritized.
- Infrastructure is designed to reduce single points of failure.
- Recovery timelines are known and achievable.

DIMENSION 2: PROTECT DATA & SYSTEMS

Controls Do Not Reduce Risk Unless They Are Validated

Security maturity is often misunderstood as the presence of tools.

An organization may have antivirus deployed, backups running, multifactor authentication configured, firewalls in place, and monitoring systems enabled. On paper, that environment may appear protected.

But protection is not defined by what has been purchased or implemented. It is defined by what is actively managed, tested, and improved.

Source: 2026 Verizon Data Breach Investigations

Across client environments, ISOutsource teams consistently see the same pattern: security controls exist, but they are not always validated. Vulnerabilities are known but not always prioritized. Monitoring tools are deployed, but not always reviewed with enough context to distinguish noise from real risk. Policies are documented but not always reflected in daily operating behavior. The gap between "implemented" and "effective" is where exposure accumulates.

This matters because the threat environment has changed. Attackers are no longer relying only on phishing emails or stolen passwords. They are increasingly exploiting unpatched systems, weak configurations, exposed applications, and trusted third-party access.

The Hidden Exposure Problem

Most organizations do not accumulate risk because they intentionally ignore security. They accumulate risk because daily operations move faster than governance.

- A system is deployed quickly to support a business need.
- A temporary access exception becomes permanent.
- A patch is delayed because the business cannot afford disruption.
- A vendor account remains active after a project ends.
- A backup job succeeds, but the restore process is never tested.

Individually, these issues are easy to rationalize. Collectively, they create an environment where leadership believes risk is managed when it is only partially understood.

Risk Assessments:
Making Exposure Visible

Risks that leadership cannot see, cannot be managed.

A structured risk assessment gives organizations a clear view of where exposure exists, how severe it is, and which risks require action first. The value is not in the findings themselves. It is in translation.

According to ISOutsource's vCISO team, Risk assessments are important because, if you're doing them right, you are translating what a weakness is from an IT perspective into an actual input for a business decision.

Without that translation, risk remains technical and decisions are delayed. Across client environments, the simplest issues are often the most underestimated.

Rapid7's 2026 Global Threat Landscape Report found that exploited high- and critical-severity vulnerabilities more than doubled year over year, while the median time from vulnerability publication to inclusion in CISA's Known Exploited Vulnerabilities catalog fell to 5.0 days.

Penetration Testing:
Validating What an Attacker Can Actually Do

Risk assessments identify and quantify the high-level risks your organization faces, but Penetration Testing shows what exposure you have to actual attacks. Both are critical in managing cyber risk.

That distinction matters.

Many organizations assume that because a vulnerability is known, it is understood. But technical awareness is not the same as business impact. A penetration test connects the dots between a weakness and a real-world outcome. It shows whether an attacker can move laterally, escalate privileges, bypass controls, or access sensitive systems under real conditions. AI is also accelerating established attack techniques, including phishing, reconnaissance, and vulnerability discovery.

> "The risks leaders underestimate the most are often the basics, like patching, system maintenance and backups because they seem small until they are documented in a risk assessment."
>
> **John Avellar**
> CISSP, CISM
> ISOutsource

Vulnerability Management:
Closing the Window Before Attackers Use It

The challenge is no longer simply identifying what needs to be patched. It is prioritizing what matters most.

ISOutsource's vCISO team reinforced the operational reality behind the research by acknowledging that what we're seeing is that one of the biggest issues is just patching your machines. We're not keeping up, and exploitation keeps growing.

They also pointed to something even more basic: **One of the simplest things to do that nobody thinks of is restarting machines**. Right now, the number one reason is not for features, it's for protection.

Rapid7 and Verizon's 2026 reporting both reinforce the same point: attackers are exploiting known exposures faster than organizations are remediating them.

KEY SIGNAL

Security activity is tied to ownership, escalation, governance, and business risk visibility.

Security Monitoring & Governance:
From Alerts to Accountability

Security monitoring is necessary, but monitoring alone is not governance.

Many organizations generate alerts. Fewer have a mature process for determining what those alerts mean, how they should be escalated, and how lessons from those alerts should inform future decisions. Without governance, monitoring becomes a reactive noise.

A protected environment does not simply detect risk. It tracks it, assigns ownership, and reduces it over time.

LEADERSHIP QUESTION

Which risks in your environment are known, documented, validated, and actively managed—and which ones are only assumed to be under control?

DIMENSION 3: PROTECT STRATEGIC DECISION MAKING

Leadership Cannot Protect What It Cannot See

Protecting an organization is not only a technical responsibility. It is a leadership responsibility.

Security tools, recovery plans, monitoring platforms, and infrastructure standards all matter. But their effectiveness depends on whether leaders have enough visibility to understand the risks, make timely decisions, and hold the organization accountable for action.

According to John Avellar, executive visibility is number one. Security has always been a top-down function. It does not work well from the grassroots.

This is where many organizations struggle. IT risk often lives below the executive line of sight until something goes wrong: a vulnerability backlog grows quietly, a vendor contract renews without review, a backup plan exists but is never tested, or a compliance requirement changes and ownership is unclear. Each of these may begin as an operational issue. Over time, they become leadership issues.

KEY SIGNAL

Leadership has regular, structured visibility into IT risk, operational resilience, and the decisions required to protect the business.

From Technical Activity to Executive Governance

One of the most common maturity gaps in IT environments is the difference between activity and governance.

Activity means work is happening. Governance means work is aligned, prioritized, documented, and accountable.

A business may have tickets being resolved, patches being applied, alerts being reviewed, and projects being completed. But if those activities are not connected to a structured decision-making framework, leadership may still lack confidence in whether the environment is actually becoming more resilient.

Governance changes the conversation from "Are we responding to issues?" to "Are we reducing the conditions that create business risk?"

The Role of vCIO and vCISO Leadership

Strategic protection requires both business alignment and security accountability.

A vCIO helps connect IT planning to business objectives.
A vCISO helps connect security decisions to risk posture.

Together, these roles help leadership answer two related questions:

1. Is our technology environment prepared to support where the business is going?
2. Is our risk environment understood, governed, and actively improving?

Without this kind of strategic leadership, IT decisions often become reactive. Projects get approved because systems are failing. Security investments are made because a client or insurer requires them. Compliance work spikes before an audit.

A vCISO provides executive-level security leadership that connects cybersecurity decisions to business risk. They build and operate the governance, risk, and compliance program, translate technical threats into business priorities, and help leadership make informed decisions that improve security, resilience, and compliance.

LEADERSHIP QUESTION

Does leadership have enough visibility into IT risk, operational resilience, vendor exposure, and security governance to make confident business decisions before disruption occurs?

"The real value of a vCIO is turning technical complexity into business clarity. Instead of reacting to outages, audits, and compliance demands, organizations gain a strategic roadmap that aligns technology investments with growth, resilience, and risk management."

Matt Gilbertson
vCIO, Director of Consulting
ISOutsource

Leadership Alignment:
Avoiding the Accountability Gap

Many IT risks persist because no one clearly owns the decision.

- The technical team may identify the issue.
- A vendor may recommend a fix.
- A department may be affected.
- Finance may control the budget.
- Leadership may need to approve the investment.

But if ownership is unclear, the decision slows down or disappears.
This creates an accountability gap. Risk remains in the environment, not because it was accepted deliberately, but because it was never formally assigned, prioritized, or resolved.

Vendor and Third-Party Oversight

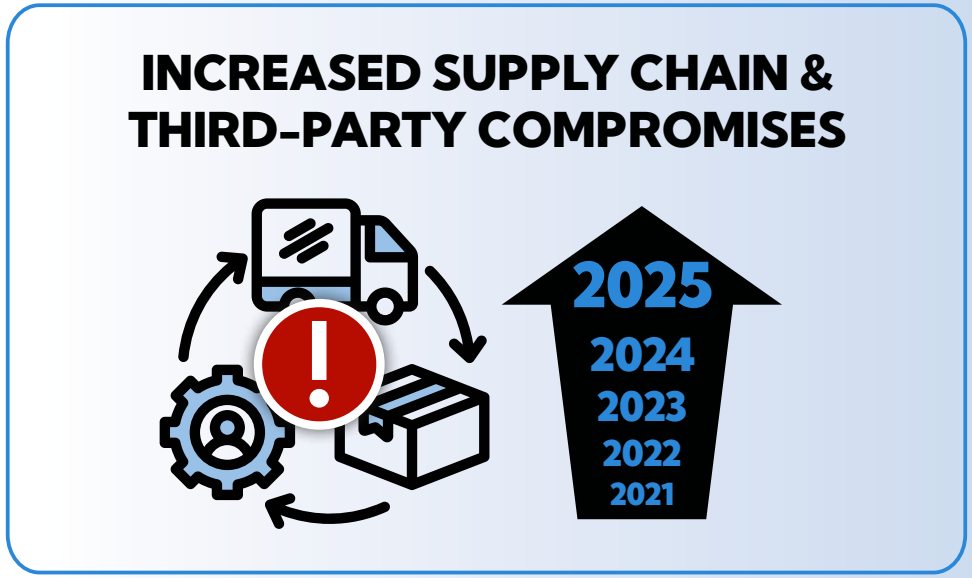
Organizations are increasingly dependent on vendors, cloud platforms, integrations, and outsourced services. Protection cannot stop at the internal environment. IBM's 2026 threat reporting notes that supply chain and third-party compromises have increased sharply over the past five years, while Verizon 2026 DBIR reporting shows breaches involving third parties rose 60% year over year and now account for 48% of breaches.

Vendor oversight is therefore not only a procurement activity. It is a security and continuity function.

Compliance Oversight

Compliance is often treated as a periodic exercise – an audit approaches; documentation is gathered, findings are remediated, and the organization moves on. But point-in-time audit readiness is not the same as operational protection.

Compliance maturity comes from discipline: the ability to demonstrate that controls are maintained, reviewed, and connected to daily operational reality.



Source: 2026 IBM Threat Intelligence Index

DIMENSION 4: PREPARING FOR AI RESPONSIBLY

AI Adoption Without Governance Accelerates Risk

AI is no longer a future planning topic. It is already entering daily operations. Employees are using generative AI to write, summarize, analyze, research, code, create, and automate. Departments are exploring AI-enabled workflows to improve productivity. Software vendors are embedding AI capabilities into platforms that organizations already use. Leadership teams are asking where AI can create efficiency, reduce manual work, improve service delivery, and support growth.

The opportunity is real. But so is the risk.

AI adoption changes how information moves through the business. It changes how employees interact with data, how decisions are supported, how work is automated, and how systems may be connected. Without governance, AI can introduce new exposure faster than organizations can see it.

> "Employees are already using AI to solve business problems. The real risk isn't AI adoption, it's adopting it without visibility, governance, or accountability. You can't manage, secure, or govern what you can't see."
>
> **Matt Gilbertson**
> vCIO, Director of Consulting
> ISOutsource

KEY SIGNAL

AI use is visible, governed, aligned to business priorities, and protected by policies, data controls, and security oversight.

The Shadow AI Problem

Most organizations will not begin their AI journey with a formal strategy. They will discover that it has already started. ISOutsource's AI Experts & Advisors point out how adoption almost always goes before executive approval.

Employees are experimenting because AI is useful. They are trying to move faster, solve routine problems, rewrite content, summarize information, and increase efficiency. But if the organization does not know which tools are being used, what data is being entered, or which workflows depend on them, AI adoption becomes unmanaged operational change.

AI Readiness Assessments:
Knowing Whether the Business Is Prepared

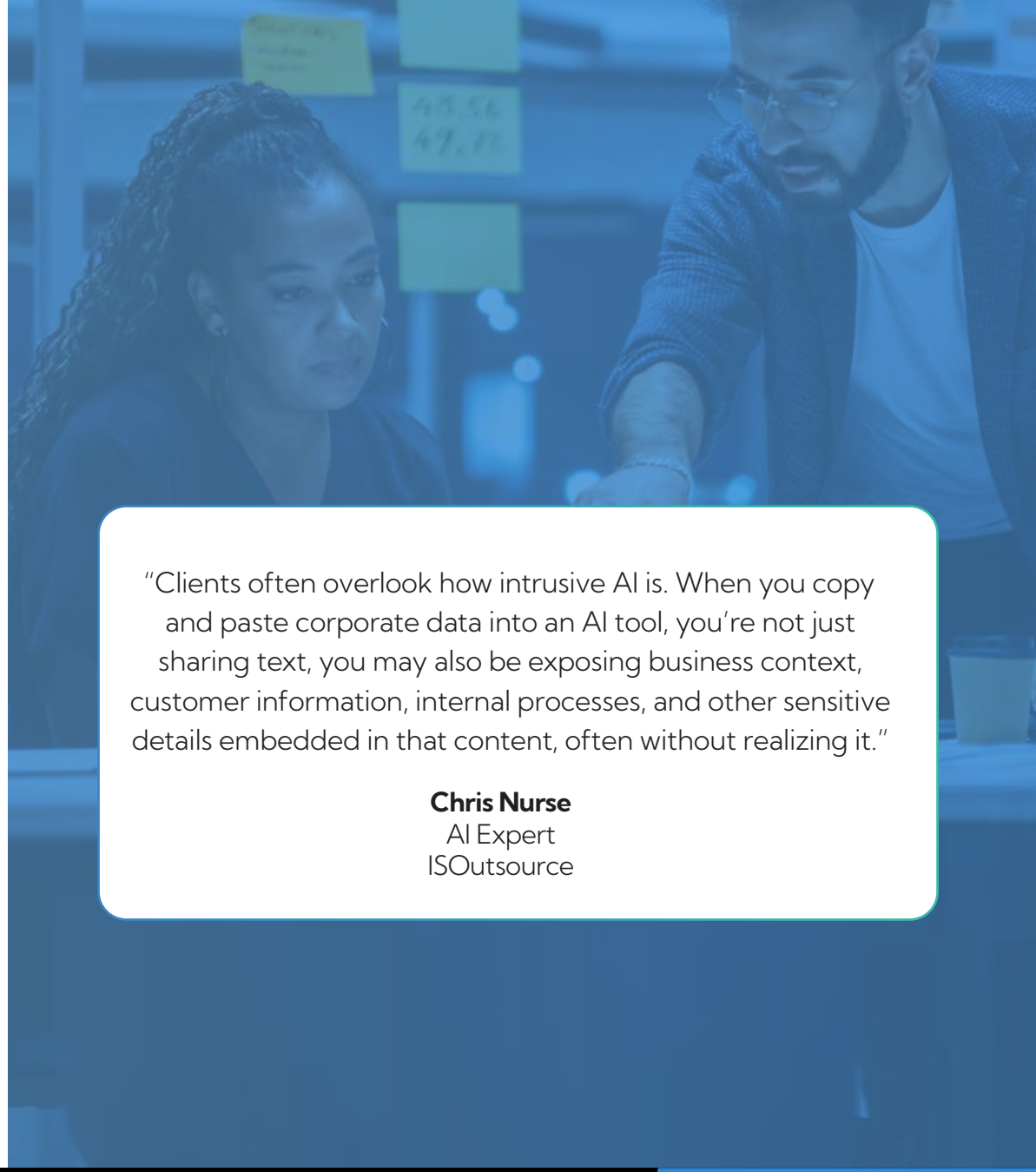
AI readiness is not a question of which tool to buy. It is a question of whether the organization has the data, access controls, visibility, and governance maturity required to adopt AI safely.

Here the risks become practical very quickly. ISO's expert team of consultants shared examples from client environments where AI readiness assessment exposed data leakage that leaders did not realize was already possible. In one biomedical organization, personally identifiable information such as bank account numbers, routing numbers, and social security numbers was already being exposed through AI-enabled systems because the environment had not been prepared correctly. In another organization, sensitive personal and health-related information was already retrievable through the tenant's AI-enabled environment even though leadership believed AI had not yet been meaningfully adopted.

These were not examples of malicious misuse. They were examples of unintended consequences.

A responsible AI readiness assessment helps leadership answer:

- Where can AI create real business value?
- What data is involved?
- What policies or controls are missing?
- Which use cases are acceptable, and which are too risky right now?



"Clients often overlook how intrusive AI is. When you copy and paste corporate data into an AI tool, you're not just sharing text, you may also be exposing business context, customer information, internal processes, and other sensitive details embedded in that content, often without realizing it."

Chris Nurse
AI Expert
ISOutsource

Data Readiness:
AI is Only as Safe as the Data Environment Around It

AI depends on data. That makes data readiness one of the most important parts of responsible adoption.

If an organization's data environment is poorly governed, AI can amplify the problem.

Unclassified data becomes easier to expose. Over-permissioned files become easier to retrieve. Outdated content becomes easier to reuse. Sensitive information becomes easier to summarize, copy, or share. NIST's AI Risk Management Framework and Generative AI Profile specifically highlights data privacy, information security vulnerabilities, information integrity, and human over-reliance as core GenAI risk categories. If you don't understand how AI works, it will just learn everything you throw at it, its like a child and it needs boundaries.

AI Governance:
Turning Innovation into a Managed Discipline

AI governance is often misunderstood as a constraint. In reality, it is what enables organizations to adopt AI at scale.

It defines how AI may be used, which tools are approved, what data can be entered, which outputs require review, who owns risk, and how adoption will be monitored over time.

This shift in framing matters. Governance is not a brake. It is the foundation that allows innovation to move faster without becoming chaotic.

"AI is only as trustworthy as what is feeding into it, the data, the tools, the connections. Governance isn't there to slow you or innovation down. It's there to give you the confidence to make sure what you're building on doesn't collapse under you."

John Avellar
CISSP, CISM
ISOutsource

Policy and Usage Controls:
Making Responsible Use Practical

AI policy has to be practical enough that employees can follow it. That means employees need clear direction on:

- Which tools are approved
- What types of data cannot be entered
- When human review is required
- What to do before AI-generated outputs are shared externally

One of the most important first steps is controlling tool sprawl.

Strong AI policy should also require people to review, translate, and validate outputs rather than copy and paste content directly into client-facing or business-critical workflows. That turns AI into a useful assistant rather than an unsupervised authority.

Responsible AI Adoption Planning

AI should not be adopted because it is novel. It should be adopted because it solves a real business problem.

Responsible planning keeps adoption grounded in measurable outcomes while ensuring that controls, access, data handling, and human review are in place first. Microsoft's 2026 Data Security Index stresses the need to pair AI innovation with robust data security, unified governance, and visibility into AI-powered workflows.

LEADERSHIP QUESTION

Is your organization prepared to adopt AI securely and strategically, or is AI already entering the business faster than your governance can manage?

"Organizations need to limit AI usage to approved solutions. Unapproved/Rogue AI tools create blind spots, introduce unnecessary risk, and make it difficult to manage, monitor, and protect intellectual property and company data."

Chris Nurse
AI Expert
ISOutsource

A Client Story: From Incident to Resilience

Restoring Operations, Rebuilding Protection

The Organization

A community-based nonprofit organization in the Pacific Northwest relied heavily on its IT systems to manage donor information, financial reporting, and daily operations. Like many small and midsize organizations, IT had grown over time without formal governance, structured security practices, or a tested recovery strategy.

The Challenge

The organization experienced a full-scale ransomware attack that resulted in a complete loss of control over its IT environment. All systems became inaccessible, operational activity stopped immediately, and a ransom demand of $200,000 was issued. The most critical issue was not only the attack itself, but the conditions that made recovery difficult: no formal disaster recovery plan, no consistent or validated backup strategy, limited visibility into system dependencies, and no structured security governance model.

The Solution

ISOutsource implemented a structured response across both recovery and long-term protection:

Immediate Actions

- Containment and threat assessment.
- Full inventory of affected systems.
- Environments rebuild across servers and workstations.
- Data recovery using the most recent available backup.

Long-Term Protection

- Implementation of backup and recovery strategies with validation testing.
- Deployment of continuous monitoring and vulnerability management.
- Establishment of patching, updates, and maintenance standards.
- Introduction of a proactive IT support model.

The Results

The organization moved from a reactive, incident-driven environment to a structured, resilient operating model. It restored operations, improved data protection and recovery readiness, reduced exposure to future incidents, and increased confidence in operational continuity.

This was not only a cybersecurity incident. It was a business continuity event.

The failure was not a lack of tools. It was a lack of preparedness, validation, and governance.

Executive Checklist: **PROTECT**

These questions are designed to help leadership teams evaluate whether their organization is prepared to operate through disruption—not just respond to it.

OPERATIONS

- Have recovery plans been tested recently under realistic conditions?
- Are all critical systems documented, prioritized, and recoverable within defined timelines?
- Do we understand how long recovery would take and what business operations would look like during that time?
- Have single points of failure been identified and addressed?
- Are backup systems validated regularly, not just running successfully?

SECURITY

- Have we completed a recent risk assessment or penetration test that reflects current threats?
- Are vulnerabilities prioritized based on business impact and actively remediated?
- Are security controls validated regularly, not just implemented?
- Do we have visibility into which risks remain unresolved, and who owns them?
- Are monitoring systems tied to escalation, governance, and decision-making—not just alerts?

GOVERNANCE

- Do leadership teams have strategic IT guidance through vCIO and/or vCISO support?
- Is IT risk visible at the executive level and connected to business decisions?
- Do we have governance policies for AI adoption, data usage, and vendor oversight?
- Are vendor relationships evaluated for both performance and risk exposure?
- Are compliance requirements embedded into operations, or addressed only during audits?

If any of these questions cannot be answered with confidence, the organization may be operating with risk that is not yet visible.

Protection is not defined by activity. It is defined by clarity, ownership, and preparedness.

Organizations that protect their environments proactively operate differently.

They do not wait for disruption to understand their risks.

They do not rely on assumptions about recovery, security, or governance.

They build structured environments where risk is visible; decisions are deliberate, and systems are prepared to operate under pressure.

Across operations, security, governance, and AI adoption, one principle remains consistent: **The cost of preparation is always lower than the cost of recovery.**

In 2026, the question is no longer whether disruption will occur. It is whether the business is prepared to continue operating when it does. Research across Verizon, IBM, Rapid7, Microsoft, and NIST all points in the same direction: attacks are accelerating, vulnerability windows are shrinking, third-party and AI-related exposure is growing, and organizations need stronger governance to maintain resilience.

Protection is not just about preventing incidents. It is about ensuring the business can recover, adapt, and move forward without lasting damage.

Organizations that do this well operate with:

- Greater resilience under pressure
- Stronger governance across systems and decisions
- Higher confidence in their ability to respond and recover

They are not just more secure. They are more capable.

In 2026, protection is not just an IT function, it is a business requirement.

ISOutsource®

Your Business–First IT Partner

500+ client engagements – 30+ years of operational experience
Washington, Oregon, Arizona

We simplify IT. We help clients save. We protect what matters.

Request a Consultation

Engage your leadership team. Build a predictable, governed IT environment that supports the business.

ISOutsource®

Where IT Means Business