REPLICA™

RESEARCH REPORT

Trading Safety for Speed: The Rise of the Exception Economy

Every Organization Is Breaking Its Own Rules

CONTENTS

01 **Introduction**
Page 1

02 **Executive Summary**
Page 4

03 **Key Findings**
Page 6

04 **Strategic Recommendations**
Page 20

INTRODUCTION

Modern work has outrun the environments built to contain it. The consequences are real: exposed intellectual property, compromised identities, failed investigations, and regulatory breaches that could have been prevented. Organizations are taking on more sensitive, complex, high-risk digital activity than ever before, and doing it on infrastructure that was never designed for what they're asking it to do. As exposure risks grow and regulatory pressure intensifies, the gap between business needs and what can be executed safely keeps widening.

This research, based on responses from 200 US cybersecurity leaders, examines where high-risk digital work is happening, how well it's protected, and what is slowing teams down. It finds that organizations are improvising across fragmented environments, approving workarounds, delaying initiatives, and abandoning roughly 1 in 5 high-risk initiatives due to exposure or compliance concerns.

These challenges aren't about lack of effort. They stem from the absence of accessible, purpose-built environments that let teams operate at the pace modern work demands. Without those environments, high-risk work stalls, and the cost shows up in delayed launches, abandoned projects, and strategic opportunities that never get off the ground.

In other words, lacking the right environment forces a choice: delay the work, cancel it, or make exceptions and proceed unsafely.

From data exposure to delayed launches to abandoned projects, each option carries a cost.

EXECUTIVE SUMMARY

Modern Workloads Are Surging into Environments That Can’t Keep Pace

Organizations are rapidly expanding their high-risk digital activities while lacking the environment, controls, and confidence to keep them secure. High-risk tasks are being carried out across a fragmented mix of environments, many of which are neither designed nor governed for sensitive operations. As a result, teams report low confidence in protecting critical assets–from IP to identities to infrastructure.

Operational friction is widespread and cuts across nearly every dimension. Tooling, infrastructure, compliance, staffing, and the risk appetite of leadership consistently block progress.

The result is measurable: 20% of high-risk initiatives are abandoned entirely, and nearly 40% of organizations have delayed market expansion, product launches, M&A, or AI deployment because the work couldn’t be done securely.

When no safe environment exists, teams resort to risky or disruptive workarounds, including using corporate systems, improvising with ad-hoc environments or using personal devices, delaying or canceling work, or outsourcing it entirely. External intelligence sharing is also heavily constrained due to fears of data leakage, legal exposure, and lack of trust.

Perhaps the clearest signal of this tension is the rise of the Exception Economy: 100% of organizations surveyed have granted security or compliance exceptions in the past year to keep high-risk work moving. Sixty-three percent do this through formal exception processes, while another 33.5% rely on informal workarounds. What were once rare exceptions have become routine, revealing a widening gap between policy requirements and operational reality. The Exception Economy is businesses trading security for speed. History suggests that’s a trade that doesn’t end well.

Taken together, the findings reveal a widening gap between how fast high-risk digital work is growing and organizations’ ability to support it securely. In the absence of purpose-built environments, teams are forced to bypass standard processes, formally or informally, to perform critical work. Over time, those bypasses become the norm, and systemic risk becomes standard operating procedure.

We trust you will find the research results illuminating.

The Exception Economy

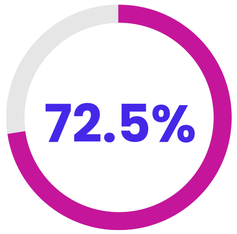
100% granted security or compliance exceptions in the last 12 months

43.5% turn to unofficial or ad-hoc environments, increasing operational and compliance risk

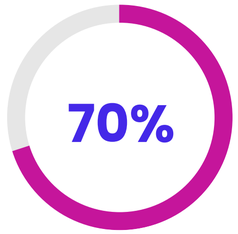
47% proceed on corporate environments, despite reservations, when no approved environment exists

20% of high-risk work doesn't go ahead owing to exposure

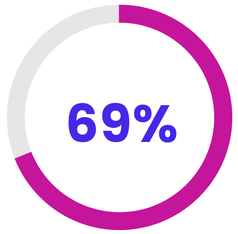
Multi-layers of blockers slow teams down



Tooling and technology limitations



Compliance restrictions



Inadequate environments

KEY FINDINGS

Organizations are running high-risk digital work on infrastructure that was never built for it, and the gap is getting harder to ignore.

The infrastructure gap is holding back growth

Organizations can't support the high-risk digital work their strategies require. Nearly 50% of respondents report that their sensitive strategic work is happening in environments that aren't fit for purpose. This slows innovation, delays revenue, and increases exposure throughout their most sensitive strategic initiatives.

High-risk work is happening across fragmented and inconsistently governed environments

Teams rely heavily on team-managed cloud accounts (45.5%) and unmanaged or ad-hoc devices (35.5%), creating uneven controls and leaving more entry points exposed.

A meaningful share of high-risk digital work never proceeds

More than half of organizations (58%) report abandoning 11–25% of potential high-risk digital activity due to exposure, compliance, or environment concerns - 20% on average across all respondents. Interestingly, the research found that CISOs pull back at nearly twice the rate of CIOs (23% vs. 13.5%), revealing a tension between security leadership and business when safe environments aren't available.

Confidence in protecting critical assets during high-risk work is low

No protection category exceeds 35.5% confidence, meaning fewer than one in three teams feel assured their IP, identities, infrastructure, or sensitive data is adequately shielded.

KEY FINDINGS

Multiple blockers are compounding

Tooling and technology limitations (72.5%), compliance restrictions (70%), and inadequate environments (69%) are each slowing teams down independently, and together they create a layered set of obstacles that's hard to untangle.

Teams are routinely forced into risky or inefficient workarounds

When no approved environment exists, 46.5% of teams proceed on corporate systems despite reservations, and 43.5% turn to unofficial or ad-hoc environments like shadow IT. CISOs, the people most responsible for security, are the most likely to proceed on corporate systems anyway (59% vs. 21% for VPs of Cybersecurity) which says something about the pressure they're operating under.

The Exception Economy: when policy can't keep up with high-risk work

Every single organization (100%) granted security or compliance exceptions in the past year, 63% did so through formal channels, and 33.5% through informal workarounds. **At that point, exceptions aren't exceptions anymore.**

An Emerging Critical Readiness Gap

The survey asked respondents which high-risk digital activities undertaken in the past 12 months could meaningfully impact their company's people, finances, reputation, or intellectual property. The results span a wide spectrum of high-risk work, but the theme is consistent: the environments organizations are using weren't built for what the business now needs to execute.

Three clear themes emerge from these responses, each pointing to the broader infrastructure gap that is slowing innovation and increasing exposure.

01 There is exposure in core strategic work

Nearly half of organizations (45%) report that their most sensitive business work, such as innovation labs, proprietary research, M&A, and high-stakes partnerships, is happening in environments that aren't fit for purpose. The exposure here is business-level: delayed deals, compromised IP, and strategic initiatives stalling at the moments they matter most.

02 Work that crosses boundaries is the hardest to govern securely

Threat intelligence, OSINT, fraud investigations, and sensitive partnerships all require information to move between teams, organizations, and vendors. Every handoff is a point where the environment gap widens, controls become inconsistent, and exposure that was contained in one place becomes someone else's problem. Sharing beyond the organization (with industry peers, intelligence platforms, or sector groups) compounds this further: 26% of organizations cite accidental data leakage as their primary barrier to external sharing, and 25.5% point to legal liability, meaning the intelligence that would most benefit the industry stays siloed.

03 AI-related activities top the list, but that's not the whole story

Legacy environments were never designed for sensitive, complex, high-risk work at this pace or scale. AI makes that gap impossible to ignore: it moves fast, touches sensitive data, and doesn't wait for infrastructure to catch up.

Fragmented Environments Are Being Used

High-risk work is happening across a wide mix of environments, most of which lack clear ownership, governance, or security oversight. Respondents report regularly using everything from team-managed cloud accounts (45.5%) to unmanaged or ad-hoc devices (35.5%), standard corporate endpoints (35%), and even contractor- or third-party-run environments (35%) for sensitive operations. Dedicated sandboxes, zero-trust workspaces, and VDI (the environments with stronger controls) are used by only about a third of organizations. The work has outpaced the infrastructure.

The results highlight how often unmanaged, third-party, or otherwise opaque environments are being used for high-risk tasks.

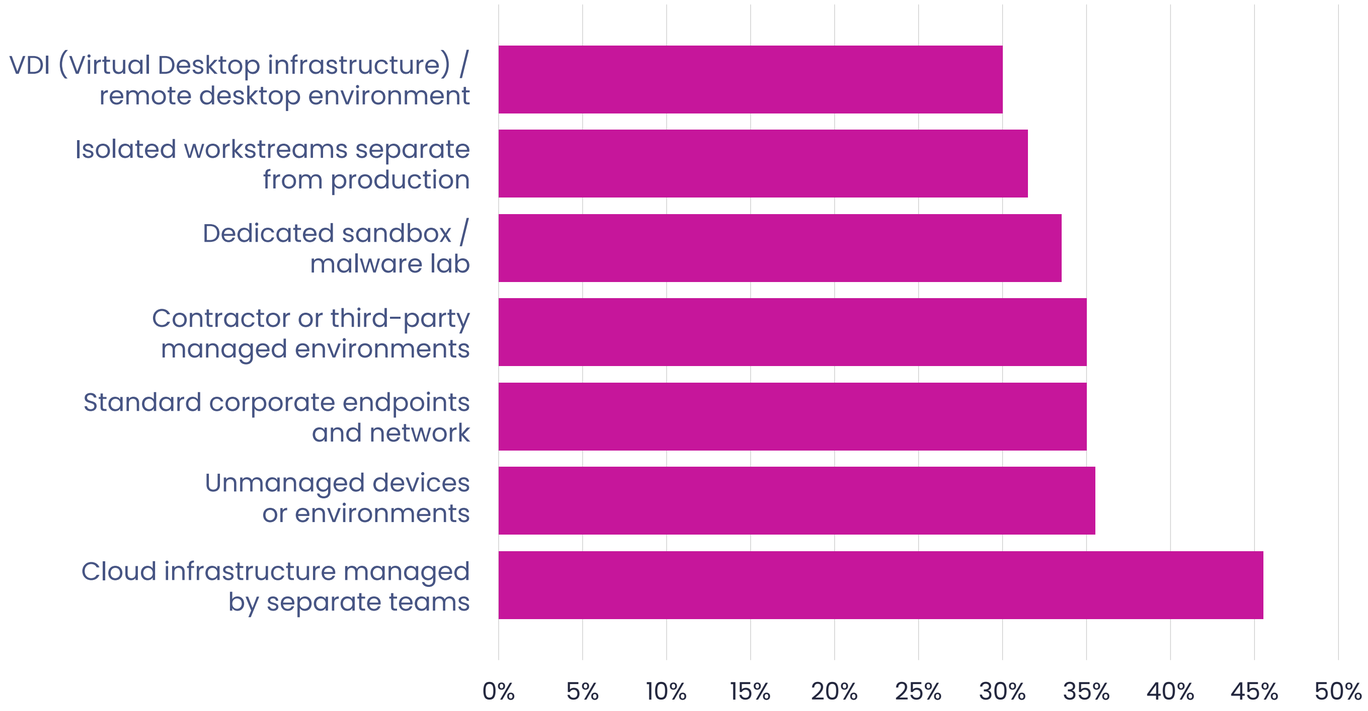


Figure 1: In the last 12 months, what environments have been used at least occasionally for high-risk digital activities in your organization?

Confidence In Protecting High-Risk Work Is Low

At best, 35.5% of cybersecurity leaders feel very confident that any single aspect of their high-risk digital work is adequately protected. Every category - IP, staff identities, devices, infrastructure - shows a vast majority of respondents have little to no confidence regarding how their high-risk digital work is protected. Every dimension of sensitive operations carries roughly the same level of doubt, with the confidence ranging just 8.5 percentage points across categories, from highest to the lowest.

Low confidence has real operational consequences. Impacts can include exposed methods that burn investigations, compromised identities surfacing in the wrong hands, sensitive data leaving corporate systems, or suspicious code affecting the network. Organizations know this, and these are the exact categories our respondents flagged as inadequately protected in their own operations.

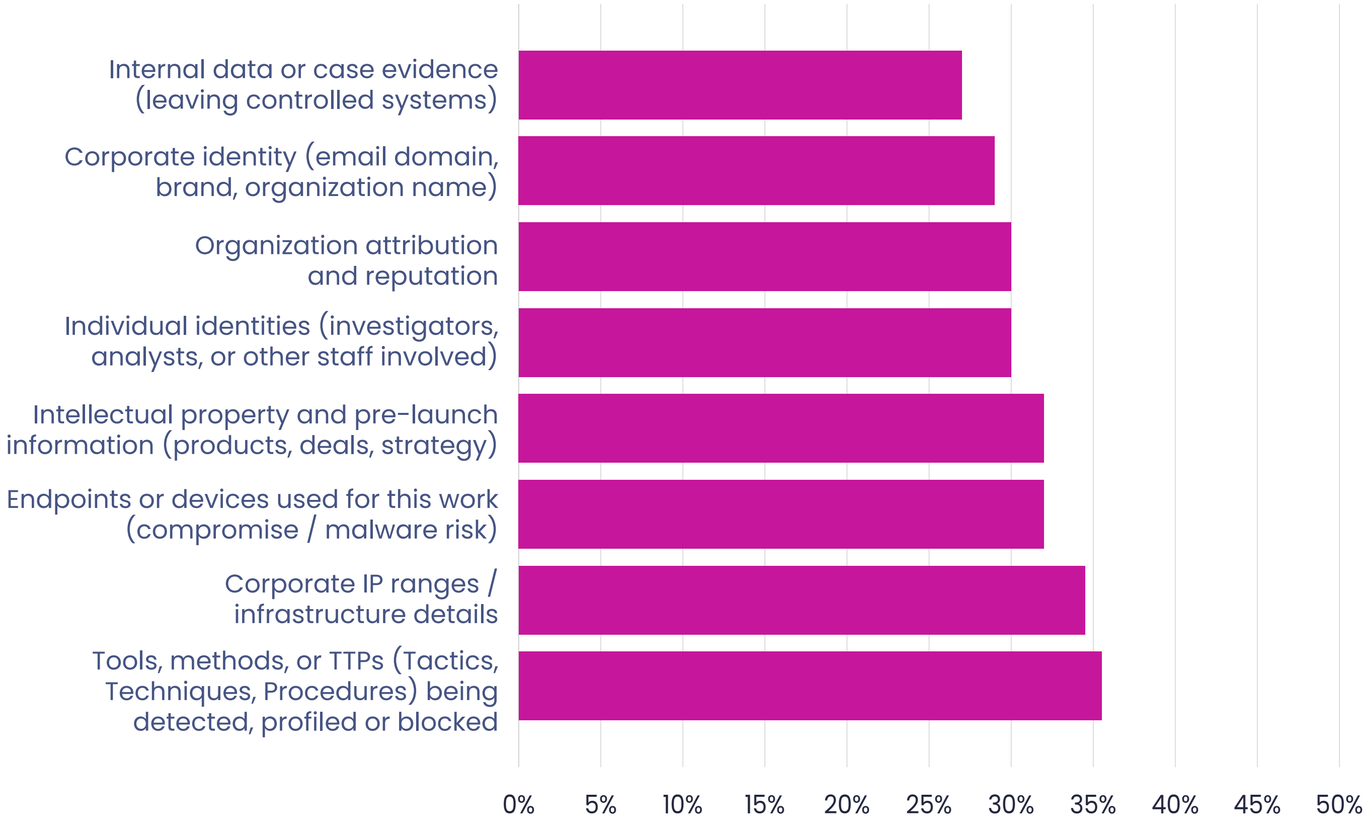


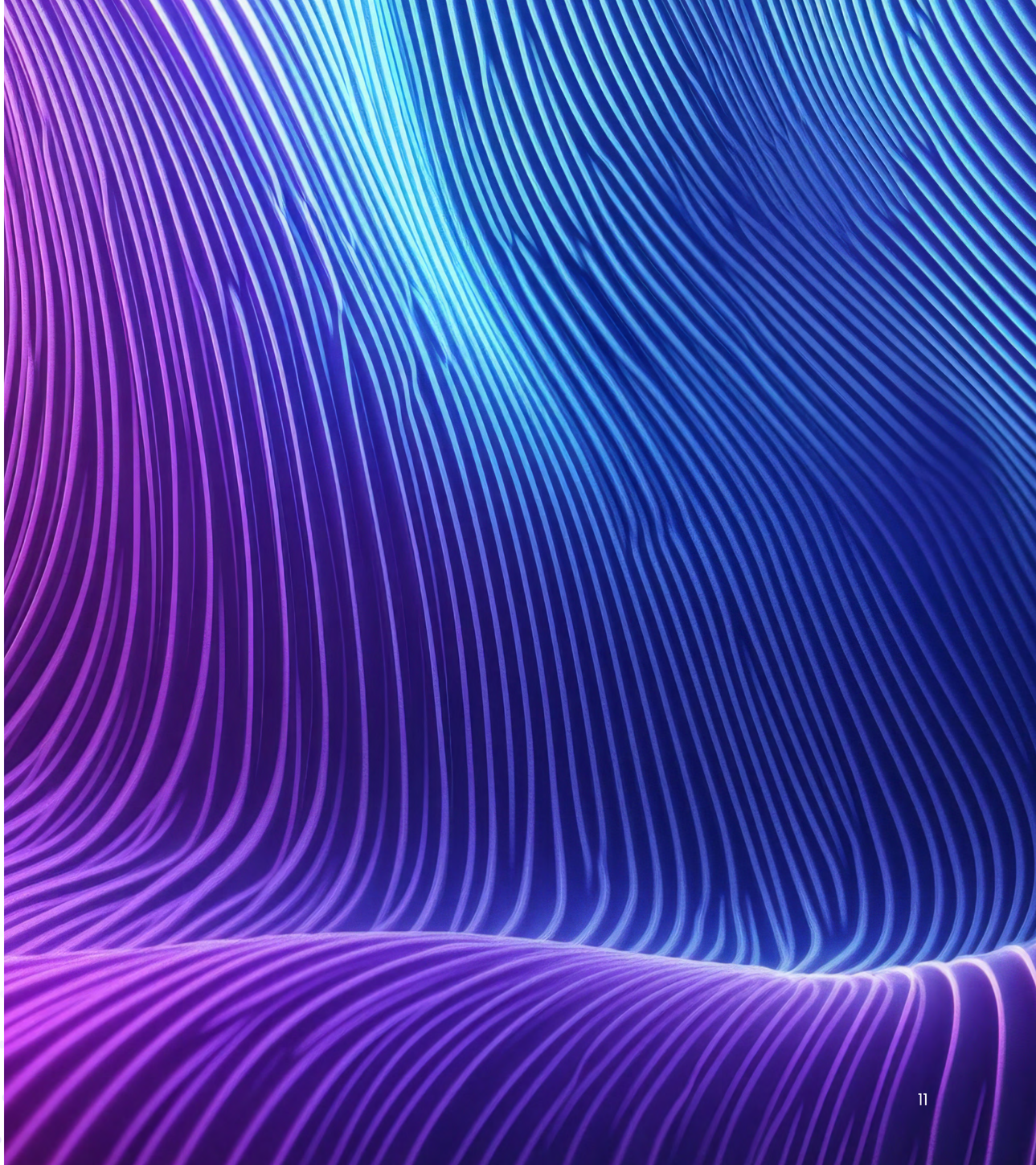
Figure 2: When your teams engage in any type of high-risk digital work, which, if any, of the following are you very confident is adequately protected from exposure or targeting?

The Cost of Being Unprepared

Roughly one in five teams say environments are not ready when needed: 20.5% report they are not provisioned before, or within an hour of, the work starting. Up to 3.5% say it takes 7 days or longer. The problem runs deeper than slow provisioning. When researchers asked VPs of Cybersecurity whether environments were ready before they were needed, the answer was yes only 5.3% of the time. Compare that to their C-suite counterparts: CISOs said yes 20.7% of the time, CIOs 20%, CTOs 27%.

Leadership doesn't see the friction that practitioners face every day.

Those delays force a choice: wait and stall the work, approve an exception to use the wrong environment, or cancel it altogether. And when leadership doesn't see delays, they may not prioritize the infrastructure to remove them.



Multiple Blockers are Slowing High-Risk Digital Work

When respondents described how often different factors limited or slowed high-risk digital activities over the past year, it highlighted that multiple blockers are both widespread and persistent. Across every dimension measured (budget, staffing, time, risk appetite, infrastructure, tooling, and compliance) most organizations, 65–75%, report these issues occurring always or often.

Tooling, infrastructure, and regulatory pressure show the highest “always” responses, running between 35% and 39%. Roughly one in three organizations considers these a permanent feature of doing high-risk digital work.

But the friction doesn’t stop there. Human and organizational factors are as limiting as technical ones. When combining “always” and “often” responses, skills shortages and leadership or legal risk appetite show similarly high levels of impact, ranking just behind tooling and technology constraints.

Overall, the data shows that high-risk digital work is being slowed from every direction, with no single constraint dominating.

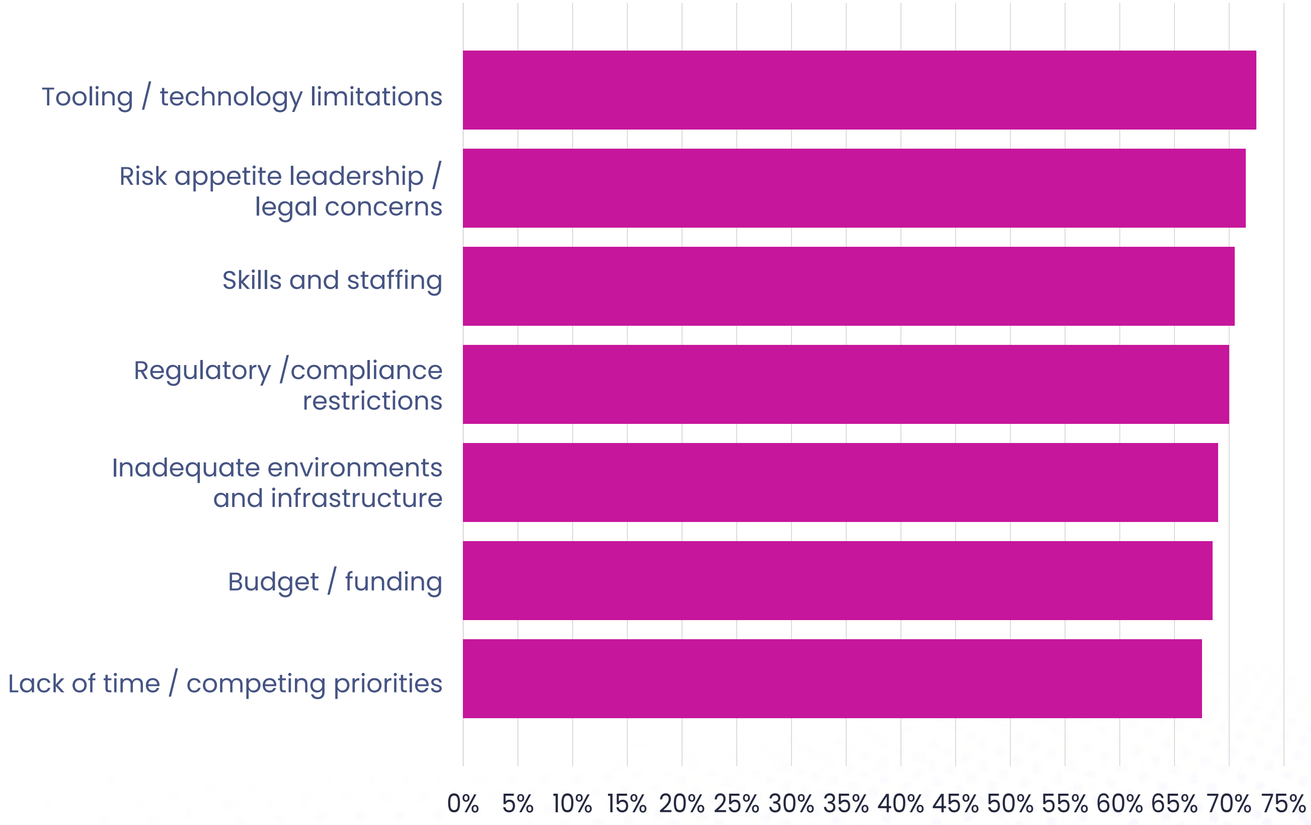


***Figure 3*: In your experience, how often, if at all, have each of the following limited or slowed down high-risk digital activities in your organization?**

Risk Concerns Are Limiting the Flow of Intelligence

Organizations want to share threat intelligence, potentially resulting in faster detection of emerging threats, reduced duplication of investigative work, and stronger collective defenses. But there are blockers.

When asked what prevents them from sharing threat intelligence or malware data with external peers, organizations pointed to three concerns clustered tightly together: accidental leakage of sensitive internal data (26%), legal or liability exposure (25.5%), and regulatory violations or contractual restrictions (24%). Negligible differences between the three suggest all are equally intimidating.

The consequences of getting it wrong – data exposure, legal action, or regulatory breach – are significant enough to make most organizations keep what they know to themselves.

Operational hurdles add to the friction: missing audit trails, uncertainty about trusted communities, and the manual effort required to safely package and anonymize artifacts before sharing. The picture is one of high caution and low trust, resulting in an industry sitting on intelligence it can’t easily move.

Data Leaks and Legal Risk Are the Biggest Barriers to Intelligence Sharing

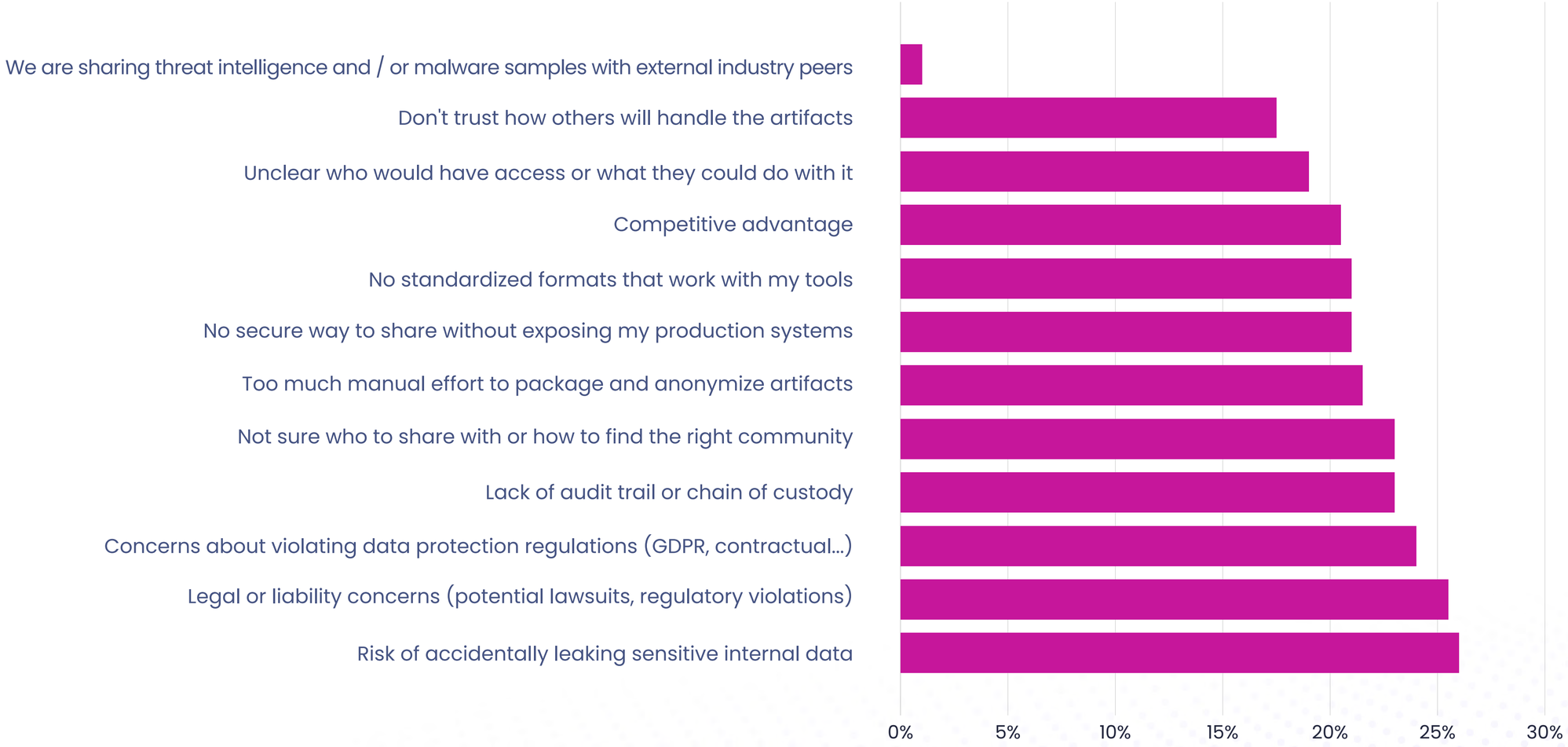


***Figure 4*: What, if anything, are the main blockers currently preventing you from sharing threat intelligence or malware samples with external industry peers (e.g. professional groups or data memberships, intelligence platforms, etc)?**

When Approved Environments Don’t Exist

What happens when teams can’t access an environment that clears the security bar for the work at hand? In those cases, there is no standard playbook. Responses scatter almost evenly across every available workaround: 46.5% proceed on standard corporate systems despite reservation about security exposures, 44% delay, reduce, or cancel the work, 43.5% shift to unofficial or ad hoc environments, and 43% push the work to third parties. The fact that these numbers are so close together tells its own story: organizations have no clear default, so everything gets attempted.

The responses from CISOs are striking. Over half, 59%, let work proceed on corporate networks even when they have reservations, compared to the just 21% of VPs of Cybersecurity who would do the same. CISOs sit closest to the business pressure to keep strategic work moving. The data suggests that proximity comes at a cost to the very standard they’re responsible for setting.

Common Workarounds for High-Risk Work

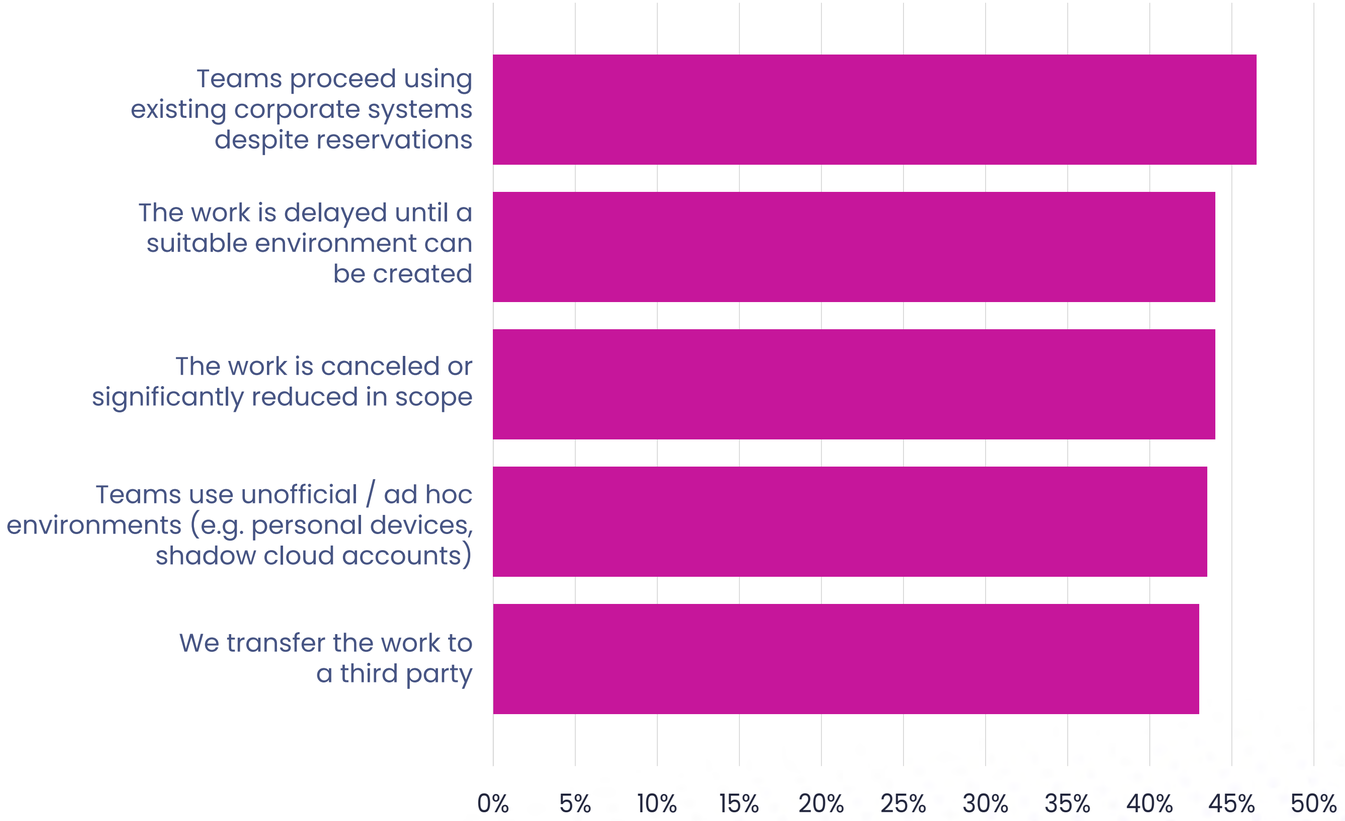


Figure 5: When there is no clearly defined or approved environment available to your team to perform high-risk digital activities, which, if any, of the following have happened in your organization in the past 12 months? (Select all that apply)

The Cost of Delay — What's Being Put on Hold?

Business activities delayed, canceled, or scaled back due to exposure, compliance, or environment concerns:

- Market expansion — **39%**
- Fraud/criminal prosecution — **39%**
- Vendor third-party onboarding — **35.5%**
- Product launches — **35%**
- M&A/strategic partnerships — **32%**

When Risk Stops Work: The Hidden Cost of Abandoned Initiatives

One in five high-risk digital initiatives never gets off the ground.

58% of organizations report abandoning between 11% and 25% of potential high-risk activity. Another 29.5% say 1–10% is blocked. With an average of 20% of work abandoned, the data shows that risk and environmental constraints are materially limiting what teams can execute. The business case exists, but the environment to do the work safely does not.

The split between roles is notable here, too, though different from the workaround data. CISOs report nearly seven times the rate of abandoned work compared to CIOs in the 26-50% range (17.2% vs. 2.5%). When two senior leaders have such different reads on the same question, the missed opportunities are likely going unnoticed by at least one of them.

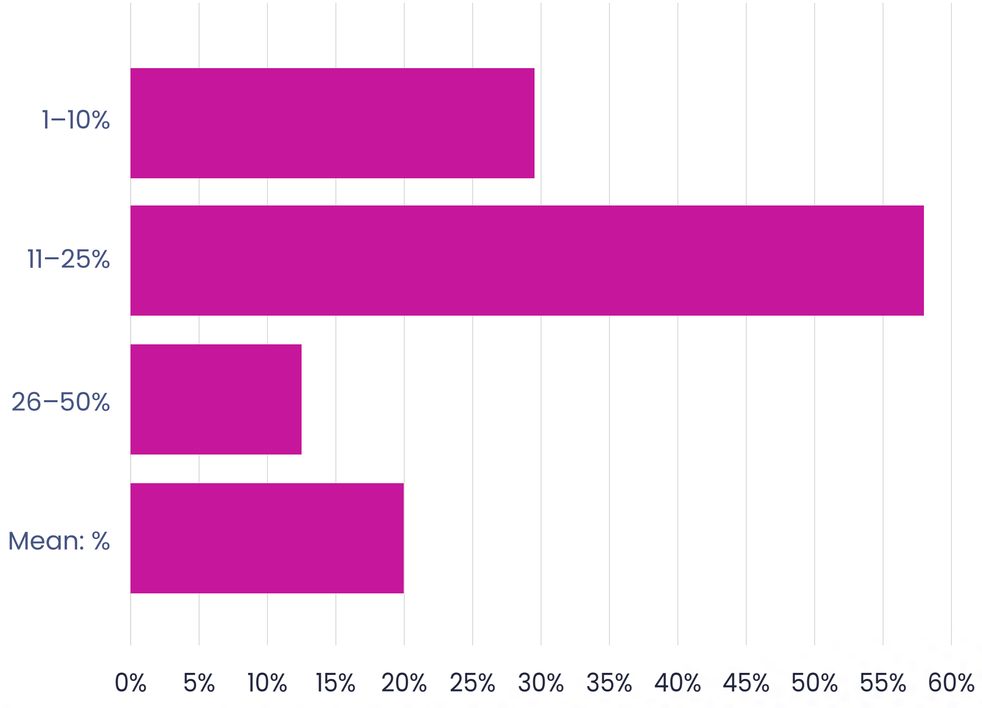


Figure 6: Approximately what percentage, if any, of high-risk digital work that your teams could be doing does not go ahead, primarily because of concerns around exposure, compliance, or having no safe environment to run it?

The Cost of Delay: When Security Gaps Stall Business Activity

When asked which business activities they had delayed, canceled, or scaled back in the past 12 months because the required work couldn't be conducted securely, organizations pointed to some of their most strategically important initiatives.

Market expansion and criminal prosecution top the list at 39% each, a pairing that speaks to how broadly security gaps affect business ledgers. Vendor onboarding and product launches follow at 35–36%, with M&A, AI/ML deployment, and regulatory approvals each affecting roughly a third of organizations. Across the board, these are the initiatives that drive revenue and growth, competitive position, and legal accountability. When they stall, the cost goes well beyond the security team's budget and reach.

A System Built on Exceptions

Every organization surveyed (100%) has granted security or compliance exceptions in the past year to allow high-risk digital work to proceed. 63% did so through formal and documented processes. Another 33.5% still rely on informal, ad-hoc approvals, like email, chat, verbal signoffs, all with limited controls and documentation. Between those two numbers, there's no organization in the dataset that truly held the line. Every exception is a control that isn't in place, and an opening that attackers don't need an invitation to explore.

When 100% of organizations have granted exceptions, the language starts to break down.

What exactly is the exception: the workaround, or the policy itself? The exception has become the rule.

The findings point to a system under pressure.

The Exception Economy has a cost in every direction: to security, to compliance, to the business initiatives that stall or never start. The way out isn't more exceptions or better documentation. It's infrastructure that makes the exception unnecessary in the first place.

STRATEGIC RECOMMENDATIONS

01 Establish secure, on-demand environments purpose-built for high-risk digital work

Teams are frequently resorting to corporate systems, ad-hoc devices, or delaying work altogether, because they are unaware that purpose-built alternatives are available. Reducing provisioning delays and eliminating unsafe workarounds requires infrastructure designed specifically for sensitive operations, not retrofitted from general-purpose IT.

02 Centralize and standardize how high-risk work is performed

High-risk activity is currently scattered across unmanaged cloud accounts, personal devices, and third-party systems. Consolidating this into a unified, governed architecture strengthens control, and gives security teams visibility while giving operators the freedom to work safely at speed.

03 Automate guardrails, controls, and auditability

Manual processes, from sanitizing data to enforcing policy, slow teams down and increase the likelihood of mistakes. Automated provisioning, access controls, logging, and chain-of-custody tracking build compliance into the workflow to reduce friction and improve audit outcomes.

04 Align security policies with operational reality

With every organization granting exceptions, and a third doing so informally, that’s a signal that policies aren’t keeping pace with how work actually gets done. Embedding controls directly into the environments where high-risk work happens reduces the gap between what policy requires, and what teams can realistically execute.

05 Enable safe, controlled intelligence sharing

Concerns about data leakage, legal exposure, and compliance are preventing organizations from sharing threat intelligence. Secure exchange mechanisms with built-in sanitization, access governance, and audit trails give teams a way to share what they know, without putting their organization at risk.

06 Build security capacity that matches business ambition

From market expansion and regulatory approvals to product launches and M&A, 39% of organizations delayed or canceled at least one of these in the past year because the work couldn't be done securely. That same security gap is what adversaries look for when organizations are moving fast on their most sensitive initiatives. Closing it is a competitive decision as much as a security one. The organizations that do it will move faster, pursue bigger opportunities, and lose less of them to risk and delay.

METHODOLOGY

Opinion Matters surveyed 200 cybersecurity leaders working in US organizations with 2000+ employees across a range of industries including construction, financial services, IT & telecoms, manufacturing and retail and healthcare. The survey was conducted in January 2026. All companies surveyed have either currently, or in the past 12 months, undertaken ‘high-risk digital activities’. This is defined as “an activity that, if something went wrong, could meaningfully impact their people, finances, reputation, or intellectual property.” Examples include sensitive business projects (strategic research, innovation lab, IP development, high-stakes partnerships, M&A, etc.), AI experimentation, AI agents or automation with some decision-making authority, threat intelligence and open-source investigations (OSINT), incident response, digital forensics, fraud and financial crime investigations, malware analysis and detonation.

About Replica

Replica is the secure environments platform for high-stakes work. It enables organizations to safely innovate, investigate, and collaborate in full isolation while protecting their data and systems. With comprehensive observability and data controls, Replica helps teams move fast, reduce security exceptions, ensure compliance, and accelerate critical initiatives.

Learn more at **replicacyber.com**