The Secure Brief

RSI NEWSLETTER

ISSUE #2606 | DATE: June 2026

June Broke Records. July Sets Deadlines.

June closed as one of the most active months on record for both attackers and patch teams. Microsoft shipped its largest security update in 23 years, supply-chain and OAuth abuse stayed the dominant entry path, and ransomware settled into an elevated new baseline.

Meanwhile, the federal compliance calendar is tightening fast. This issue covers what mattered, what is changing, and what to prepare for now.

The most damaging incidents this year were not exotic. They traced back to third-party access, unpatched systems, and over-permissioned identities.

From the RSI Security Desk

Two forces define this month. Attackers are moving faster, and regulators are responding. CISA's own framing is blunt: AI is helping both researchers and adversaries find software flaws, vastly increasing the pace at which new vulnerabilities are discovered, and defenders are already struggling to keep up. The federal compliance calendar is tightening in parallel, with CMMC Phase 2 now four months out.

The throughline is preparation over reaction. The organizations with the most leverage are not the ones with the most tools. They are the ones already in motion, with accurate inventories, disciplined patch cadence, and compliance treated as a continuous posture rather than a once-a-year event.That is the lens for everything in this issue.

rsisecurity.com

By the Numbers: 2026 Verizon DBIR

For the first time in the report's 19-year history, vulnerability exploitation has overtaken stolen credentials as the leading initial-access vector, accounting for 31% of breaches.

Third-party supply-chain involvement jumped 60% year over year and now factors into 48% of all breaches. Ransomware appeared in 48% of breaches, up from 44%, even as 69% of victims declined to pay. The human element remained present in 62% of breaches.

The reason third-party risk keeps climbing is structural. Only 23% of third-party organizations fully remediated missing or improperly secured MFA on cloud accounts, and weak passwords and permission misconfigurations took a median of eight months to resolve half of all findings.

Your data lives in those environments. Their remediation pace becomes your exposure window.

Source: Verizon 2026 Data Breach Investigations Report, analyzing 22,000+ confirmed breaches across 145 countries.

What Will be Inside Of The Newsletter

THREAT LANDSCAPE

What Defined June 2026

June reinforced a pattern that has held all year. The most damaging incidents are not exotic. They trace back to third-party access, unpatched systems, and over-permissioned identities. Adversaries are now using AI to compress the time between a published vulnerability and a live exploit to mere hours, which turns routine patch lag into material risk.

Active Exploitation to Act On

CISA added a critical remote code execution flaw in PTC Windchill PDMLink and FlexPLM to its catalog, and as of June 25, PTC confirmed continued reports of heightened exploitation activity. A Linux kernel privilege-escalation flaw nicknamed "pedit COW" also saw a working public exploit appear within a day of disclosure, a reminder of how compressed the patch window has become.

Ransomware's New Normal

Volume is holding at elevated levels rather than spiking, but the operator landscape is shifting. A relatively new group, The Gentlemen, expanded from 35 victims in late 2025 to 182 in early 2026, becoming the second most active group, while established operators Qilin and Akira declined 25 and 22 percent. Across the board, attackers increasingly favor data theft and extortion over traditional encryption. Lower operational complexity, the same pressure on the victim.

The Record Patch Tuesday

On June 9, Microsoft released its largest security update since the Patch Tuesday program began 23 years ago, fixing 206 vulnerabilities, 39 of them rated Critical. Roughly 65 were elevation-of-privilege flaws, the category attackers most often chain into the early stages of an intrusion. Remote Desktop Client was the single largest cluster at 11 CVEs. The cycle also patched multiple Secure Boot and BitLocker bypasses, continuing a pattern of attackers targeting pre-boot integrity and full-disk encryption. If your patch cadence is monthly, this cycle warranted an out-of-band review.

Supply Chain and OAuth Abuse

Third-party access remained the dominant path in. The Klue and Salesforce OAuth campaign attributed to the Icarus group exposed CRM data across multiple organizations, including several cybersecurity firms. Separately, the ShinyHunters group claimed to have compromised Oracle PeopleSoft servers at more than 100 organizations, with the bulk of victims being colleges and universities. The lesson echoes federal guidance. Vendor-mediated access continues to be identified as a leading attack pattern, and building vendor oversight into the security program is no longer optional for organizations handling regulated data.

The takeaway. Patch velocity, an accurate asset inventory, OAuth and third-party app review, and least-privilege access remain the highest-leverage controls. None are new. All are still where breaches start.

Reflects reporting from CISA, The Hacker News, Arctic Wolf, eSecurity Planet, and GuidePoint as of late June 2026. Threat data evolves quickly; verify specifics before external citation.

ACROSS THE CYBER REALM

Signals Worth Tracking

01

AI on Both Sides

The DBIR's AI findings this year are notably grounded rather than speculative. Verizon collaborated with the Anthropic Safeguards Team to analyze 793 threat actors flagged for misuse, finding the median threat actor used AI assistance across 15 distinct MITRE ATT&CK techniques. Of AI-assisted initial access, 44% mapped to phishing and 32% to exploiting vulnerabilities. The verdict is measured: AI is a force multiplier on known craft, not a paradigm shift, automating and scaling techniques defenders already know how to detect.

02

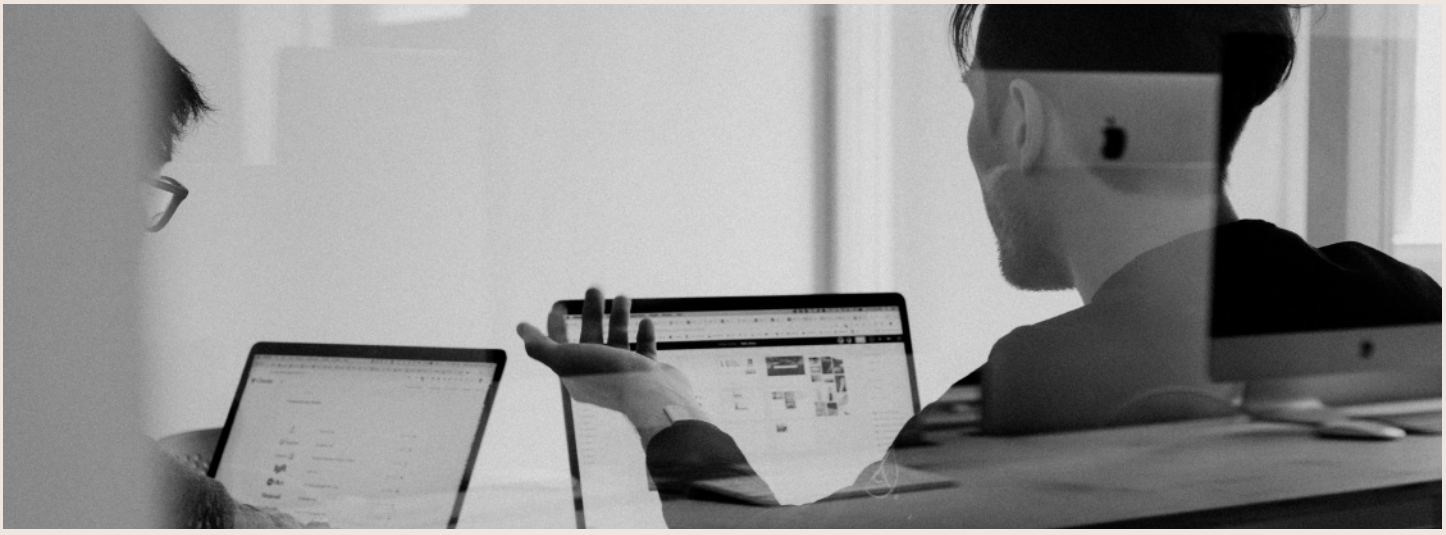
Identity Debt From AI Adoption

Shadow AI is now a measurable exposure, not a hypothetical. Regular AI use among employees climbed to 45%, up from 15% the prior year, and 67% of users access AI services from corporate devices using non-corporate accounts. Shadow AI became the third most common non-malicious insider action in Verizon's data-loss-prevention dataset, a fourfold increase in a single year. Combined with autonomous agents left running after their creators move on, the result is a governance gap that most security stacks were never designed to see. You cannot secure what you have not inventoried.

A coordinated law enforcement operation with Bitdefender, Bitsight, ESET, and Microsoft disrupted the infrastructure behind the Amadey and StealC malware families and recovered roughly 27 million stolen credentials.

Critical Infrastructure

The data backs the model. Only 26% of CISA Known Exploited Vulnerabilities were fully remediated in 2025, down from 38% the year prior. Third-party vendors take a median of eight months to resolve half their identity-hygiene findings. Point-in-time assessments cannot see the drift that happens in those gaps. **Continuous monitoring can.**



Your Compliance Partner

RSI Security is a trusted leader in cybersecurity and compliance, helping organizations of all sizes strengthen defenses, meet regulatory requirements, and maintain resilience in an evolving threat landscape.

Through Continuous Digital Safeguard Services (CDSS), we deliver proactive monitoring, incident response, compliance management, and ongoing program optimization, all built around your organization's unique environment and risk profile.

Our multidisciplinary team combines deep expertise in threat detection, vulnerability management, regulatory compliance, and incident response to provide complete protection that grows with your business.

From assessment to automation, RSI Security simplifies cybersecurity, empowering your team to focus on what matters most: innovation, growth, and customer trust.

SERVICE HIGHLIGHT

Security That Does Not End at the Assessment

Continuous Digital Safeguard Services (CDSS)

This month's spotlight is on the philosophy that runs through everything RSI Security does. The assessment is the starting line, not the finish. Most organizations treat compliance as a point-in-time event. Prepare, assess, exhale. The smarter approach treats it as a continuous posture.

CDSS is built for the gap between audits, the months where threats evolve, environments drift, and evidence goes stale. It pairs continuous control monitoring with senior advisory support, so the work invested in readiness keeps compounding rather than decaying.

For teams managing overlapping frameworks, that means evidence and documentation structured for reuse across future audits, certifications, and compliance efforts. The result is reduced rework and shorter future assessment timelines.

This is what Partnership Beyond the Assessment means in practice.
Embedded advisory continuity, not a report handed over and a door closed.

1 **Real-Time Protection**

Detect and neutralize threats instantly with 24/7 monitoring, analytics, and automated response.

2 **Continuous Compliance**

Maintain alignment with frameworks like NIST, HIPAA, PCI DSS, and CMMC through ongoing assessments and policy updates.

3 **Scalable Efficiency**

Adapt coverage to your evolving environment & gain enterprise-grade protection.

4 **Lower Operational Costs**

Reduce total cost of ownership by consolidating tools, automation, and expert oversight under one unified service.

JULY 2026

Where the Industry Gathers

A lighter month than the August Hacker Summer Camp stretch, but a few relevant gatherings.

July 20 **FLGISA Annual Conference 2026**
Aventura, FL
Florida's local-government IT conference, with a strong focus on cybersecurity and digital services. Relevant for organizations serving SLED clients or pursuing state and local government work, where compliance expectations increasingly mirror federal frameworks.

July 22–24 **Gartner Security & Risk Management Summit**
Tokyo, Japan
Gartner's APAC security summit, covering AI governance, shadow AI, cyber-risk management, cloud security, and threat-detection automation. Primarily relevant for organizations with international operations or APAC-region compliance obligations.

> *Any college has quite a few departments, who are often not on the same page when it comes to IT or security. RSI Security met with vendors, partners, and internal sta and made sure everyone understood what needed to happen and how to make it happen.*
>
> **Mike Zimmerman CIO**
> Executive Director of Communications & IT
> Macomb Community College

REGULATORY SPOTLIGHT

CISA Rewrites the Rules on Patching

The biggest federal cybersecurity development of June was not a breach. It was a directive. On June 10, 2026, CISA issued Binding Operational Directive 26-04, telling federal civilian agencies to prioritize security updates based on risk using four concrete signals: whether the asset is publicly exposed, whether the vulnerability is in the KEV catalog, whether exploitation can be automated, and whether a breach would give an attacker total system control.

The shift is meaningful. When all four boxes are ticked, agencies have just three days to remediate and must perform forensic triage to determine whether they were already compromised; lower-risk combinations receive 7, 14, or 30 days, or deferral to the next regular upgrade.

Why it matters beyond government: the directive codifies what mature enterprises already do, and the data explains the urgency. Only 26% of vulnerabilities on CISA's Known Exploited Vulnerabilities catalog were fully remediated by organizations in 2025, down from 38% the prior year, while the median time to full resolution rose to 43 days. CISA also adds a sharp reminder that applying a patch generally does not evict a threat actor, so checking for existing compromise is vital.

For private-sector organizations, the move is a template. Federal agency policies must be updated by August 7, 2026, with full use of the new timelines by December 7. Regulated industries should expect this risk-based model to shape audit and procurement expectations well beyond the .gov domain.

Source: CISA, Binding Operational Directive 26-04, June 2026.

Sonia Agnesod

Planning, Coordination, and Compliance

Empowering a Mission-Driven Nonprofit with PCI DSS Assessment Support

USA for IOM demonstrated alignment with applicable PCI DSS requirements within the defined assessment scope and established a stronger foundation for managing compliance responsibilities independently. Key outcomes included:

1) Secure acceptance of digital donations as an independent nonprofit Increased donor confidence and readiness for future fundraising growth

2) Robust policies and documentation aligned to industry best practices

3) Clear understanding of renewal timelines and vendor expectations

4) Quarterly vulnerability scanning and long-term compliance planning

Most importantly, the organization emerged more confident, prepared, and informed as it continued to scale its digital fundraising capabilities.

"They Didn't Just Guide Us — They Partnered With Us.

Despite our limited technical knowledge, RSI made the process approachable by explaining requirements in plain language and helping us understand what was needed from our vendors and systems."

PARTNER HIGHLIGHT

IntelliGRC

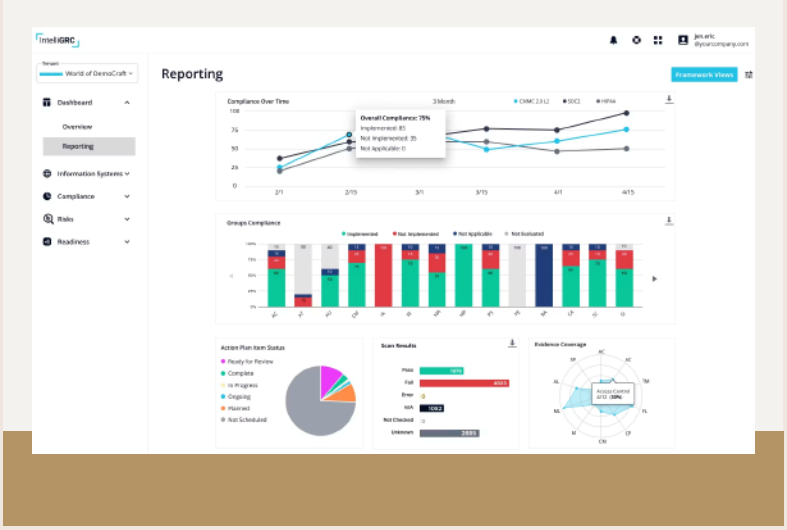
This month we are spotlighting IntelliGRC, a governance, risk, and compliance platform purpose-built for the realities of stringent cyber frameworks, and a valued RSI Security partner in the CMMC and continuous-compliance space.

IntelliGRC is a provider-first GRC platform, built by practitioners, to streamline compliance with CMMC, NIST 800-171, SOC 2, ISO 27001, HIPAA, and more, using asset-centric scoping, expert-calibrated AI, and auditable outputs. It maps cleanly to the frameworks that matter most to RSI Security's clients, including CMMC, NIST 800-171, NIST 800-53, FedRAMP, HIPAA, ISO 27001, SOC 2, and PCI DSS.

The platform is trusted by many CMMC Third-Party Assessment Organizations for smoother assessments, and it automates control mapping, evidence collection, and continuous compliance. That directly reduces the manual documentation burden that slows most readiness efforts. For organizations heading into a Level 2 assessment, accurate asset-centric scoping and automated evidence mapping address two of the most common sources of audit friction: incomplete scope and disorganized evidence.

IntelliGRC closed a 3.5 million dollar seed round in early 2026, co-led by Huntress co-founder and CEO Kyle Hanslovan and Blu Ventures, to deepen its AI capabilities and expand across the service-provider ecosystem.

Together, RSI Security and IntelliGRC turn CMMC from a confusing obligation into an operational advantage, pairing practitioner-led advisory with purpose-built compliance automation.



At a Glance: IntelliGRC

AI-native cybersecurity GRC platform purpose-built for the Defense Industrial Base. FedRAMP Moderate Equivalent, and trusted by many C3PAOs for smoother CMMC assessments.

Frameworks: CMMC · NIST 800-171 · NIST 800-53 · FedRAMP · HIPAA · ISO 27001 · SOC 2 · PCI DSS

Built for: Asset-centric scoping, automated evidence mapping, and continuous control monitoring.

C3PAO capacity is finite. As Phase 2 takes effect, the organizations with the most leverage are the ones already in motion.

UPCOMING TRANSITIONS

What Is Changing Across Our Services

CMMC

CMMC Phase 2 enforcement begins November 10, 2026. This is the deadline every defense contractor should have circled. Phase 2 introduces CMMC Level 2 C3PAO certification assessment requirements for most contracts involving Controlled Unclassified Information. C3PAO capacity is finite, and demand will surge as the date approaches. With Level 2 readiness typically requiring six to twelve months, the window to start is now. RSI Security holds direct C3PAO authorization; per 32 CFR Part 170 independence rules, our advisory and assessment teams operate separately.

HIPAA

HIPAA Security Rule update remains pending, not yet in force. An important correction to any mid-2026 forecasts: as of late June 2026, the proposed HIPAA Security Rule overhaul has not been finalized, and OCR's targeted spring window has passed with nothing published. OCR continues to enforce the current rule. When finalized, the proposal would mandate encryption of ePHI at rest and in transit, require multifactor authentication, and require an asset inventory that explicitly lists AI tools handling ePHI. The right move for healthcare organizations is to prepare now, not wait for publication.

AI & PCI

ISO 42001 and NIST AI RMF: the governance window is opening. AI governance budgets are forming rather than flowing, but organizations building readiness now will lead when budgets unlock. RSI Security provides ISO 42001 and ISO 27001 advisory and readiness services, not certification. Separately, PCI DSS 4.0.1 is fully in force; RSI Security holds QSA and ASV designations directly.

The Secure Brief

Partnership Beyond the Assessment

RESOURCES

New For Your Organization

1. **Preparing for FedRAMP?** Check out our new readiness checklist to get your organization ready from an outside 3PAO assessor.
2. **Cyber Maturity Scorecard.** See where your program stands across people, process, and technology in roughly five minutes.
3. **Unified Federal Compliance Roadmap.** A plain-language guide to navigating CMMC and FedRAMP together, built around the November Phase 2 runway.
4. **AI Governance Readiness Guide.** Build a defensible program across ISO 42001, NIST AI RMF, and HIPAA before AI tools become mandatory inventory line items.
5. **Weekly Threat Report.** The short-form companion to this monthly brief, tracking the threats that matter as they break.

Where to Start

If one theme runs through this issue, it is that the fundamentals still decide outcomes. An accurate asset inventory, disciplined patch prioritization, third-party and OAuth visibility, and compliance built to sustain rather than expire are not advanced moves. They are the baseline, and they are still where most breaches begin.

RSI Security helps regulated organizations turn that baseline into a defensible, continuous program, from CMMC and FedRAMP readiness to AI governance and continuous cyber maturity, with advisory continuity that does not end when the assessment does.

YOU HAVE QUESTIONS

Our Team Has Answers

info@rsisecurity.com
Southlake, TX
rsisecurity.com
(858) 252-2448