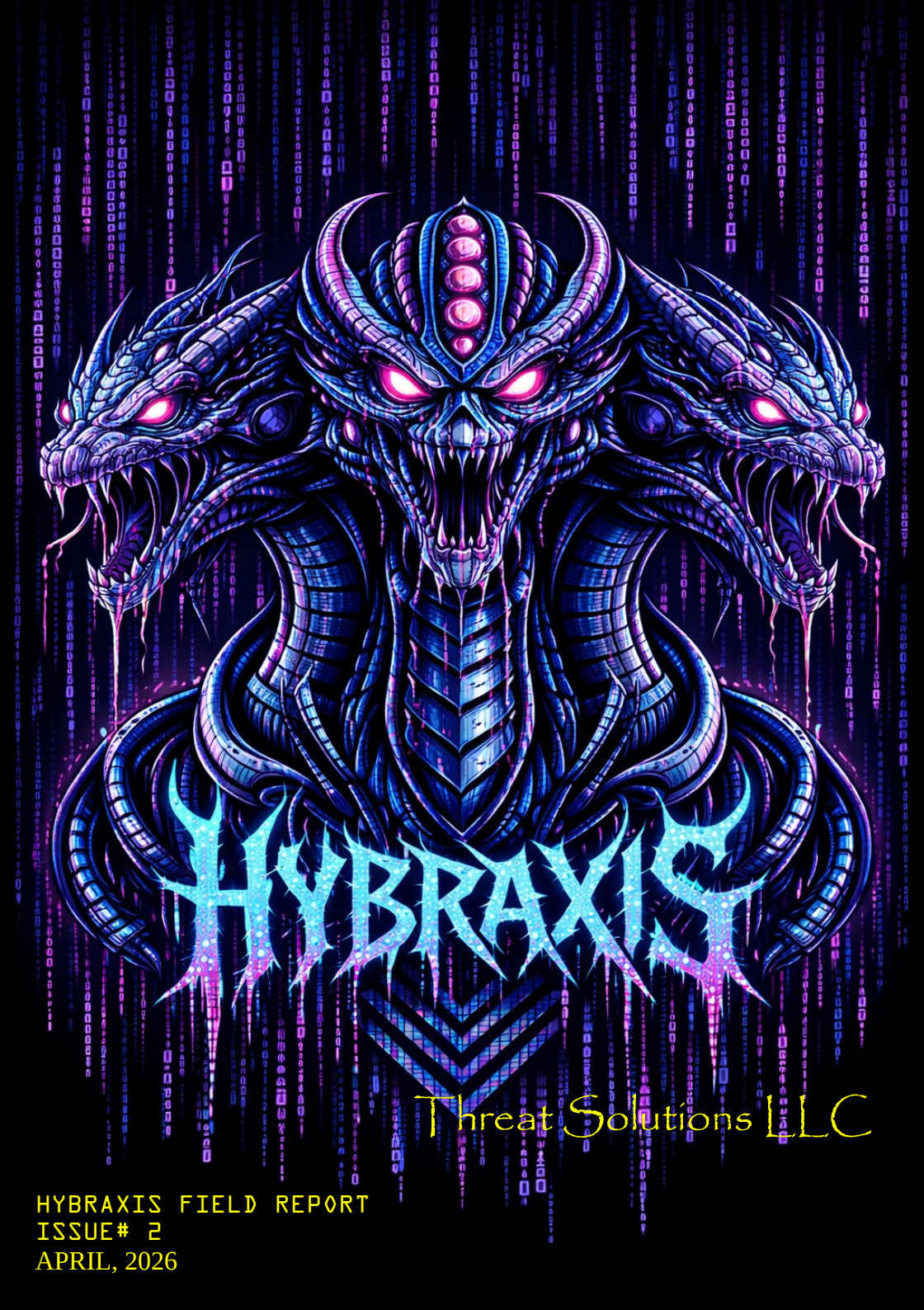

HYBRAXIS FIELD REPORT
ISSUE# 2
APRIL, 2026

HYBRAXIS FIELD REPORT

This is not a comfort publication.

It is a field guide to the systems watching you.

This is about the machinery.

How metadata becomes intelligence.
How habits harden into predictive models.
How convenience disguises extraction.
How anonymity erodes quietly — without announcement, without consent.

You are not breached once.
You are accumulated continuously.

We examine the infrastructure beneath the interface:

Data brokerage markets.
Machine classification pipelines.
Platform telemetry.
Signal interception.
The convergence of corporate and state surveillance.

No tinfoil. No theatrics.

Just structure.

Security culture sells tools and aesthetics.
We study power and architecture.

You do not need to be technical.
You need to be willing to look.

This is a quarterly, independent zine from Hybraxis Threat Solutions LLC.

Signal is never neutral.
Question everything.
Assume collection.

Welcome to the field.

Quarterly. Independent. Feedback welcome.

A NOTE TO THE READER

The *HYBRAXIS FIELD REPORT* is released quarterly. Each issue dives into the systems shaping your digital life — independent research, operational breakdowns, and adversarial analysis.

Want to contribute an article? Prefer to read digitally? You can also receive a **free PDF version via email**. Just send a request to: **hybraxisthreatsolutions@gmail.com** (Subject: "PDF MAILLIST")

We create this zine for those willing to look closer. Choose your level of engagement, but always read critically.

Welcome to the field.

— The Hybraxis Threat Solutions Team

Hybraxis Threat Solutions LLC — P.O. Box #2, Calhan CO 80808
Need Cyber security Consulting?
hybraxisthreatsolutions@proton.me

(see back for details)

Inside This Issue

Passwords+lazy = millions lost and what happens to your digital footprint after your untimely demise? We bet Zuckerberg profits. Also we take a look at what it takes to be CMMC/NIST compliant in today's competitive DOD landscape.

- Passwords Your Digital Lifeline — and Your Longest Graveyard
- Ghosts in the Machine Your Social Media Will Outlive You
- The NIST situation

////////////////////////////////

Passwords: Your Digital Lifeline-And Your Longest Graveyard

Passwords date back to ancient times. For instance in Rome soldiers used watchwords at gates to identify themselves and in medieval times, castles and military camps had secret codes or "passwords" for access. Oral or written, simple, shared among trusted people. Security relied on secrecy, not encryption. Early computing brought passwords that were typically stored in plain text and were rudimentary. Unix (1970's) introduced hashed passwords using cryptographic techniques, increasing security. By the time networking systems and the rise of the internet age, things had already gotten complicated. Dictionary attacks became common. Password storage still had flaws; early hashing methods could be brute-forced. And salting (adding random data to hashes) became standard to protect stored passwords. Fast forward to today, and the threat landscape progresses further each year then anyone thought possible. In **2025 there were about 12,195 confirmed data breaches globally, the highest number ever recorded in a single year. In 2024, global account breaches reached well into the billions (over 5 billion breached user accounts). On average a cyberattack occurs about every 39 seconds worldwide, a metric often used to approximate breach-related incidents. (demandsage.com Data Breach Statistics (2026) - Trends, Costs & Impact). What do they all have in common? What is the common denominator? Human error.

From our standpoint (Hybraxis Threat Solutions), its a very straightforward solution to a very complicated nuanced situation. Its point A to point B. The problem(s) arise when businesses/organizations or individuals have to introduce convenience in their security posture. Let us be the first to say this if you haven't heard it before; "Security isn't convenient, and convenience isn't secure". The solution is simple, people are not. If you do the following you are ahead of 90 percent of the computing population.

Use 16+ character passwords (longer is better). (We prefer 32 when possible)
• Make every password unique — no reuse.
• Use a password manager •
Turn on multi-factor authentication (MFA) — prefer hardware keys (e.g., Yubico).
• Regularly check for breaches and change exposed passwords

And make no mistake about it, in 2026 if your excuse for getting hacked is "I don't know how to use a computer", "I'm not a computer person", "I'm to old to learn"…you need to stay off the devices. Put em down. We are here to tell you...This mentality is no longer cute, its a war out there and the bad actors aren't

playing around anymore...Here's some more stats for my baseball nerds out there.

Rough Modern Estimates (Ballpark) for data breaches/hacks

Target	*Typical Impact*
Individual	$500–$5,000+ direct loss
Small business	$50,000–$500,000
Large enterprise	$3M–$5M+
Major breach	Tens or hundreds of millions

Passwords were never meant to matter this much. What began as a simple shared secret between a human and a machine now serves as the guardian of bank accounts, private communications, healthcare records, cloud archives, and fragments of identity that could persist long after you're gone. They outlive us. They do not decay. They linger in databases, backup servers, and cloud caches, quietly waiting, inert yet alive in code. Modern attackers exploit this persistence. They don't guess manually in dark basements; they deploy clusters of GPUs, FPGAs (field programmable gate arrays), and optimized ASICs (application specific integrated circuits), ripping through password hashes at rates that make human cognition irrelevant. An 8-character password hashed with a fast algorithm like MD5 or SHA-256 can fall in minutes; a 12-character password might survive a few years depending on hashing, but once you reach 32 characters, you enter a realm of practical impossibility — even against the most massive GPU clusters.

Length is exponential power. Every additional character multiplies the keyspace, turning brute force into something closer to a thought experiment than a feasible attack. But length alone is not enough. Hashing functions determine how efficiently attackers can test guesses. Fast hashes (MD5, SHA-1, SHA-256) allow billions of guesses per second on commodity hardware. Slow, memory-intensive hashing like bcrypt (high cost factor) or Argon2id converts every single guess into a resource-taxing operation, slowing attackers by orders of magnitude. Salt adds a second layer of protection, ensuring precomputed attacks and rainbow tables fail. Without these protections, even a strong password can become trivial once leaked in a database breach.

AI doesn't attack your password directly, but it dismantles the human element. Large language models can craft thousands of context-aware phishing emails per second, generate realistic AI-generated voice messages, or create malicious AI-powered chatbots that mimic colleagues, friends, or corporate systems. One misclick, one misplaced trust, and your carefully constructed password is in the wrong hands. Credential stuffing compounds the problem. When one breach exposes a password, automated tools attempt the same credentials across multiple platforms. Reused passwords are a silent apocalypse waiting to happen. Unique, random passwords paired with hardware multi-factor authentication (MFA) are your only sanctuary.

Quantum computing is the horizon you cannot ignore. While large-scale quantum machines capable of breaking cryptography remain largely

theoretical, attackers can harvest encrypted data today and store it indefinitely — a strategy known as "harvest now, decrypt later." Grover's algorithm, which could theoretically halve the entropy of symmetric keys, highlights the importance of long, high-entropy passwords. Even under future quantum advances, 32-character random passwords remain astronomically resistant to brute-force attacks. The lesson is clear: defenders buy time; attackers buy persistence and patience. Time is the true currency of survival.

Password storage is as crucial as password choice. Slow, memory-hard hashes like Argon2id, or high-cost bcrypt, ensure that each guess is computationally expensive. A single hash evaluation may cost milliseconds, but multiplied across billions of guesses, it becomes a wall of time and resource cost. Salts ensure uniqueness across systems, making precomputed attacks useless. Together with 32-character high-entropy passwords and hardware MFA, these defenses transform password protection from fragile hope into near-impenetrable reality. Yet humans remain the weakest link. AI-driven social engineering exploits curiosity, urgency, fear, or greed, bypassing brute force entirely. Your password's strength counts only if you do not willingly hand it over. In practice, this means embracing extreme measures. Use a password manager to generate 32-character random passwords for every account. Avoid reuse. Enable hardware MFA wherever possible. Assume your accounts will always be targeted by automated AI systems and social engineers. Choose hashing functions and algorithms that slow the attacker to impractical speeds. And remember: your password does not age or decay; it accumulates risk over time. The digital afterlife is patient. Attackers are patient. Survival requires that you be exponentially more prepared than anyone else.

Passwords were never meant to carry this much weight — yet today they stand between order and chaos in a world where attacks are automated, scaled, and relentless. The technology will continue to evolve. GPUs will get faster. AI will get smarter. Quantum may one day arrive. But the fundamental truth will not change: security is a choice made daily, deliberately, and without excuses. Length. Uniqueness. Hardware-backed authentication. Discipline. These are not advanced tactics — they are the baseline for survival. The organizations and individuals who endure will not be the most convenient; they will be the most consistent. In a threat landscape that compounds every year, resilience is not built on hope or optimism — it is built on preparation. And preparation, unlike regret, is always cheaper.

R Sturdevant, April: 2026 Feedback & mailing list: hybraxisthreatsolutions@gmail.com (Include "Passwords: Your Digital Lifeline — and Your Longest" in the subject line)

References DemandSage. (2026). Data Breach Statistics (2026) – Trends, Costs & Impact. https://www.demandsage.com/data-breach-statistics/ IBM Security. (2024). Cost of a Data Breach Report 2024. IBM Corporation. Shannon, C. E. (1949). Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4), 656–715. NIST. (2023). Digital

Identity Guidelines (SP 800-63B). National Institute of Standards and Technology. OWASP Foundation. (2023).

////////////////////////////////

Ghosts in the Machine: Your Social Media Will Outlive You

We used to worry about dying and being forgotten. Now the problem is the opposite. You will die. Your Facebook probably won't. Your birthday reminders will keep firing. Your tagged photos will remain searchable. Your old jokes will sit quietly in comment threads. Algorithms will keep resurfacing "memories" like digital séances nobody asked for. We are the first generation to leave behind terabytes of ourselves. When someone dies, their body is handled with ritual, legality, and ceremony. Their data, however, is something else entirely.

Social platforms all handle death differently. Some memorialize accounts. Some lock them. Some require documentation. Some simply allow the account to sit there, slowly decaying into inactivity. And here's the uncomfortable truth: if no one reports your death, your account just lingers. Inactive, but not gone. A profile picture floating in the system. A presence without a pulse. The internet does not understand grief. It understands engagement. That means your face might reappear in "People You May Know," anniversary reminders, AI-generated slideshows, or automatic tag suggestions. To a machine, you are data with historical interaction weight. To your family, you are a ghost in their notifications. What many people don't realize is that loved ones do not automatically gain access to your accounts after you die. Passwords die with you unless you planned otherwise. Many platforms require formal processes, proof of death, and legal documentation before changes are made, and even then access is often limited.

So what happens to your private messages, your cloud storage, your draft emails, your unfinished notes, the photos no one else has? They continue to exist. But they may never be seen. Digital archaeology is real — and often impossible. Now we are entering even stranger territory. AI systems can be trained on your writing style, your messages, your voice recordings. With enough data, a system could simulate a version of you that responds the way you might have. Is that comforting? Or is it a chatbot wearing your skin?

Consent becomes murky when the person who could grant it is gone. The ethics remain unsettled. The technology continues moving forward. We may soon live in a world where death is biological, but presence is optional. Your online identity is a second self. It does not age properly. It does not decompose. It simply freezes at the last update. In a hundred years, archaeologists may not dig up bones; they may scrape servers. And perhaps the most unsettling part is this: most of us have not decided what should happen to our digital remains. We obsess over passwords while alive, yet almost no one writes a digital will. We built a kind of immortality by accident. We just did not think about the haunting.

-G.R.Quinonez
Feedback & mailing list:
hybraxisthreatsolutions@gmail.com

(Include "Ghosts in the Machine" in the subject line)

////////////////////////////////

The NIST Situation:

Companies in the United States that work with the federal government, particularly within the defense supply chain, are required to comply with Special Publication 800-171 issued by the National Institute of Standards and Technology. Known as NIST SP 800-171, this framework establishes mandatory cybersecurity controls for protecting Controlled Unclassified Information (CUI) that is stored, processed, or transmitted by non-federal organizations. The requirement is not theoretical or advisory; it is embedded in federal contract law through mechanisms such as the Defense Federal Acquisition Regulation Supplement (DFARS) and applies broadly to contractors and subcontractors supporting the U.S. Department of Defense. If a company handles sensitive federal data, compliance is a condition of doing business with the government.

The framework itself contains 110 security controls across 14 domains, including access control, incident response, configuration management, encryption, multifactor authentication, audit logging, and continuous monitoring. These controls are not abstract recommendations; they are concrete technical and administrative safeguards that must be implemented and documented. Historically, contractors were allowed to self-certify compliance, but that era has shifted toward verification and oversight. Formal assessments and third-party validations now play an increasing role in determining eligibility for contract awards.

Failing to meet these requirements carries serious ramifications. A company that cannot demonstrate compliance risks losing current contracts and being deemed ineligible for future federal work. For organizations heavily dependent on defense revenue, this can represent an existential threat. Even more severe are the legal implications of falsely claiming compliance. Companies that attest to meeting NIST 800-171 requirements without actually implementing them may face liability under the False Claims Act, exposing them to federal investigations, whistleblower actions, and potentially treble damages. Financial penalties can reach into the millions, and executive leadership may come under direct scrutiny.

At its core, NIST SP 800-171 reflects a stark reality: cyber conflict is ongoing, and private companies that handle federal information are part of that battlefield whether they recognize it or not. Compliance is costly and often disruptive, but the alternative—lost contracts, federal enforcement actions,

and long-term exclusion from the defense market.

Where Companies Actually Fail: A Technical Look at High-Risk Controls:

For many contractors, the moment NIST compliance becomes real is not when the regulation is published, but when an auditor begins asking questions. What initially appears to be a checklist of security practices quickly turns into a detailed examination of how systems actually operate. Assessors do not simply ask whether encryption or logging exists; they ask where logs are stored, who reviews them, how administrative access is protected, and whether vulnerability scans are followed by documented remediation. Evidence becomes the currency of the audit process—screenshots, system configurations, ticket histories, and security policies that demonstrate controls are not only written but actively enforced.

It is in this phase that many organizations discover the difference between having security tools and operating a compliant security program. The following controls are among the most technically demanding and most frequently scrutinized during federal cybersecurity assessments.

While NIST SP 800-171 contains 110 individual controls, auditors and federal assessors tend to focus on a smaller subset that consistently causes organizations to fail evaluations. In practice, the most scrutinized requirements are those that are technically complex, operationally demanding, or difficult to implement across legacy environments. Data from assessments across the defense industrial base shows that failures rarely occur because companies misunderstand the policy; they occur because implementing security controls across real infrastructure—mixed operating systems, legacy software, industrial systems, and cloud services—is far more difficult than the framework's language suggests.

One of the most frequently scrutinized requirements is multifactor authentication under Control 3.5.3. NIST requires multifactor authentication for privileged accounts and for remote access to systems handling controlled information. While many organizations deploy MFA for VPN access or cloud applications, auditors regularly find gaps in internal administrative systems, legacy platforms, and service accounts. Administrative credentials without MFA, privileged accounts shared across multiple administrators, and systems that bypass identity enforcement are common findings during assessments. These weaknesses are particularly serious because authentication controls sit at the center of modern intrusion techniques; once attackers obtain administrative credentials, most other security controls become irrelevant.

Encryption requirements also generate significant compliance challenges, particularly under Control 3.13.11, which requires the use of cryptography validated under the Federal Information Processing Standards program. Many organizations assume that using common encryption protocols such as TLS or AES automatically satisfies the requirement, but the standard is more specific than that. The cryptographic modules themselves must be validated under federal standards and often must operate in FIPS-validated mode. In practice, auditors frequently discover systems using non-validated libraries, outdated VPN firmware, improperly configured endpoint encryption products, or applications relying on embedded cryptographic code that has never undergone validation. Because encryption is used across so many layers of infrastructure—file transfers, databases, storage systems, VPNs, and web services—verifying compliance requires tracing cryptographic implementations throughout the entire environment.

Audit logging and event monitoring requirements are another frequent failure point. The audit and accountability domain requires organizations to generate, retain, protect, and review logs capturing security-relevant activity across their systems. Enabling logging alone is not sufficient; organizations must demonstrate that logs are centralized, protected against modification, and regularly reviewed for suspicious behavior. Many companies collect large volumes of system logs but lack centralized analysis tools or defined procedures for reviewing them. During an assessment, auditors often ask for evidence that log review actually occurs —such as alert records, security tickets, or documented analysis. When organizations cannot demonstrate that monitoring is an active operational process rather than a passive data collection effort, the control is typically considered unmet.

Vulnerability management and patch remediation also present ongoing operational challenges. Control 3.14.1 requires organizations to identify system vulnerabilities and correct them in a timely manner, which generally involves automated vulnerability scanning, patch management systems, and documented remediation timelines. The technical difficulty lies not in scanning systems but in maintaining a disciplined remediation process across hundreds or thousands of assets. Assessors frequently find environments where vulnerability scans are performed but the results are not consistently tracked, prioritized, or resolved. Large backlogs of critical vulnerabilities, unsupported software, and unpatched systems are common findings in organizations that lack a structured vulnerability management program.

Risk assessment and continuous monitoring controls similarly require ongoing activity rather than one-time

documentation. NIST requires organizations to periodically evaluate risks to systems handling controlled information and update security measures accordingly. However, many companies produce a single risk assessment document to satisfy compliance requirements and rarely revisit it. During audits, assessors may ask how organizations have updated their threat models in response to new attack techniques, supply chain compromises, or major ransomware campaigns. If the assessment process is not continuous and demonstrably tied to security improvements, the requirement is generally considered incomplete.

Across these domains a clear pattern emerges. ***The controls that organizations struggle with most are those that require continuous operational capability rather than static configuration***. A firewall rule or encryption setting can be implemented once, but processes such as monitoring logs, patching vulnerabilities, enforcing multifactor authentication, and conducting risk assessments require constant execution. Many organizations initially believe they are compliant because the necessary tools exist within their environment. It is only during a formal assessment—when auditors begin requesting operational evidence—that the difference between possessing security technology and actually operating a compliant security program becomes apparent.

Understanding these controls—and more importantly, implementing them in a way that withstands scrutiny during an assessment—requires more than simply installing security tools or drafting policy documents. Organizations must translate the language of NIST SP 800-171 into operational systems, enforceable procedures, and verifiable evidence that controls are functioning as intended. For many companies in the defense supply chain, particularly small and mid-sized contractors, that translation process can be complex and resource-intensive. If your organization is preparing for a NIST 800-171 or CMMC assessment and needs assistance designing, implementing, or validating these controls, our team specializes in helping contractors build compliant security environments that meet federal requirements while remaining practical to operate. -The Hybraxis Team

If you need help cutting a path to NIST compliance, we specialize...

//////////////////////////

About Hybraxis Threat Solutions LLC ////////////////////////////

Hybraxis Threat Solutions LLC operates where risk is real and excuses don't exist. Built on decades of operational experience and hardened by the realities of both physical and digital threat environments, Hybraxis brings an operator's mindset to modern security challenges. We don't theorize problems — we confront them, dismantle them, and leave clients stronger than we found them.

Our approach is deliberate, disciplined, and uncompromising. Whether guiding organizations through complex compliance frameworks, delivering high-impact training, or engineering tailored protection strategies, Hybraxis executes with precision and finality. We believe security should be decisive, measurable, and done right the first time. This isn't checkbox consulting. This is operational security thinking applied to the environments where failure has consequences. ***Hybraxis Threat Solutions — Do it or Don't.***

services we offer:

Offensive Operations:

Internal & External Penetration testing
Physical security testing
Phishing simulations
Full-scale red teaming exercises
Social engineering simulations

Compliance & Remediation :

Nist 800-171/CMMC lvl 1-3 mock audits/ gap analysis/ remediation
HIPAA compliance/guidance/mock audits
NIST/HIPAA-Compliant IR Tabletop Exercises
Role-Based Access Control Review

Training & OSINT

Executive Cybersecurity Workshops
Quarterly Cybersecurity Awareness Training (NIST)
Customized Workshop (Half-Day)
Cybersecurity Awareness Training (Group Session)

Defensive & OSINT

Internal & external vulnerability scans
WiFi Auditing
M&A; (Mergers & Acquisitions) or Background Screening
Executive OSINT Scrub
Ongoing Monitoring & Removal

We do general Consulting as well...if you don't see what your looking for...ask.

////////////////////////////////

For security and consulting email us at:
hybraxisthreatsolutions@proton.me