NSSF®
The Firearm Industry Trade Association

PROJECT CYBERSAFE

MEMORANDUM

The Assumed-Coverage Gap

What firearms industry businesses should expect from their managed service provider, and how to confirm they are receiving it

PREPARED IN PARTNERSHIP WITH

fellsway

October, 2026 | Draft for NSSF review

MEMORANDUM

TO: NSSF Members, Project Cybersafe
FROM: Fellsway, in partnership with NSSF
DATE: October, 2026
RE: **Working with Managed Service Providers: The Assumed-Coverage Gap**

EXECUTIVE SUMMARY

Many firearms industry businesses rely on a managed service provider for technology, and many assume that relationship covers cybersecurity. Frequently it covers only part of it. The contract defines what the provider is responsible for, and everything outside that definition stays with the business.

This memorandum traces how that gap forms and where it tends to appear, explains how responsibilities divide between a managed service provider (MSP) and a managed security service provider (MSSP), and sets out a practical path to close the gap using the Project Cybersafe Quick Guide.

Key points for members

- Accountability for protecting firearms transaction records, customer data, payment data, and export-controlled information remains with your business, whoever performs the work.
- An MSP keeps technology running. An MSSP watches for and responds to threats. Whether a member needs one, the other, or both depends on its environment and obligations, and on who will act when an alert fires overnight.
- Evidence beats assurance. A restore test, an MFA coverage list, and a list of every account with admin rights reveal more than any monthly status report.
- A short written record of each gap, and the decision made about it, converts hidden risk into a choice leadership has made deliberately.

The gap usually surfaces in a single conversation. Ransomware has encrypted a retailer's systems over a holiday weekend, and the owner asks the MSP why no one caught it sooner. The MSP, accurately, points to the agreement: after-hours monitoring was quoted three years earlier as an add-on and never purchased. Nothing the provider did was wrong. The two sides had simply been working from different readings of the same contract, and neither had checked.

The Project Cybersafe Quick Guide on Working with MSPs exists to prevent that conversation. The sections that follow explain the reasoning behind it, written for owners and managers of manufacturers, distributors, and retailers rather than for IT staff.

How the gap forms

An MSP agreement is a scope document. It lists the services the provider will deliver, the systems it will manage, and the response times it commits to. Anything not written into that scope is, from the provider's point of view, out of scope. That is a reasonable way to run a services business. It becomes a liability when the client assumes "managed IT" includes "managed security."

Several things widen the gap over time. Agreements are often signed when the business is smaller, before it added e-commerce, a second location, or a government contract. The MSP's standard offering may include antivirus and patching but treat email filtering, log monitoring, or security awareness training as paid add-ons that were never purchased. Staff turn over on both sides, and the person who understood what was and wasn't covered leaves. Meanwhile, the owner receives a monthly report full of green checkmarks and reasonably concludes that things are fine.

Many providers do solid work within the boundaries they were given. The gap is a communication failure more often than a competence failure, and it is fixable once both sides can see it.

Why the stakes are higher in the firearms industry

Firearms industry businesses hold data and carry obligations that many small businesses do not. Retailers maintain federally required transaction and acquisition records, handle customer identity information, and process card payments. Manufacturers may hold technical data subject to export controls, and those supplying the Department of Defense face contractual cybersecurity requirements, including CMMC/NIST SP 800-171 r2/r3. Nearly every business in the industry is also subject to state data breach notification laws, and many face heightened public and media attention when an incident occurs.

Accountability for these obligations does not transfer to the MSP. You can outsource the work, but a regulator, prime contractor, card brand, or insurer will look to you when something goes wrong. For that reason, the Quick Guide asks whether your MSP understands what your organization is obligated to meet. An MSP that has never been told you handle export-controlled drawings cannot be expected to protect them accordingly.

The provider relationship itself also creates risk. An MSP holds administrative access to every client it serves, usually through remote monitoring and management tools. Attackers know this. The 2021 attack on Kaseya's VSA platform pushed ransomware through MSPs to well over a thousand downstream businesses in a single weekend, and CISA and its international partners issued joint guidance in 2022 warning that MSPs had become a preferred path into small and mid-sized organizations. When you hire an MSP, its security posture becomes part of yours.

What the gap looks like in practice

A few patterns come up repeatedly in the assessments Fellsway performs.

Backups that have never been restored. The report says every job completed successfully. No one has tried to bring the business back from those backups under realistic conditions, so no one knows whether it takes four hours or four days, or whether the backups were stored somewhere the ransomware could also reach. A completed backup job and a working recovery are different facts, and only a restore test establishes the second one.

MFA in some places but not others. Multi-factor authentication is on for email, so the box gets checked. Remote access into the network, the MSP's own admin accounts, or the firewall management console may still sit behind a password alone. Those are exactly the doors attackers try first.

No plan for the first hour of an incident. An MSP's incident response plan typically covers its own technical actions and little else. Who notifies the insurer? Does the insurer require its own incident response firm, which may need access your MSP controls? Who decides whether to shut down systems, and who speaks to customers? When these questions are answered for the first time during an incident, hours are lost and insurance coverage can be put at risk.

Exit costs nobody priced in. A business decides to change providers and discovers an early termination clause close to the full remaining contract value, licenses held in the MSP's name, and no defined process for returning data or credentials.

Tools and third parties the owner doesn't know about. MSPs run on a stack of platforms and sometimes subcontract parts of their work. Each one is another party that can touch your systems. More recently, many providers have adopted AI-assisted tools for ticketing, documentation, and troubleshooting, and some of those tools ingest client data. Adoption is moving faster than most MSPs' ability to document how that data is handled, retained, or used for model training. Few owners have thought to ask.

MSP, MSSP, or both

Members evaluating outside support will encounter two kinds of provider that sound alike and do different jobs. Understanding the distinction before speaking with vendors prevents a common mistake, which is buying one while expecting the other.

The distinction is sharper than the names suggest. An MSP's security work is mostly hygiene, such as patching, antivirus, and basic firewall administration, performed as part of keeping systems running. An MSSP's entire purpose is detecting and responding to attacks, and it rarely touches day-to-day IT.

How the two models compare

	MSP (Managed Service Provider)	MSSP (Managed Security Service Provider)
Core job	Keep systems running, users productive, and technology current.	Detect, investigate, and help contain security threats.
Typical services	Help desk, device and server management, patching, backups, network administration, licensing, and vendor coordination.	Security monitoring (SIEM), managed detection and response (MDR/EDR), threat hunting, vulnerability scanning, firewall monitoring, and incident support.
Coverage hours	Usually business hours, with after-hours support for outages.	Typically 24x7 through a security operations center (SOC).
Staff focus	Generalist IT technicians and engineers.	Security analysts and incident responders.
Measured by	Ticket response times, uptime, and user satisfaction.	Time to detect, time to contain, and alert quality.
Common blind spot	Security controls outside the contracted scope, and no one watching logs overnight.	Usually limited to detection and containment; remediation such as patching or rebuilding typically falls to the client or its MSP.

Weighing the options

Neither model is better in the abstract; each covers ground the other does not. A business with only an MSP is well maintained but, unless monitoring is contracted, largely unwatched after hours. A business with only an MSSP receives alerts and still needs someone to act on them.

The workable arrangements include an MSP alone with security written into its scope, an MSSP alongside an in-house IT team, two firms working in a co-managed model, a single MSP that delivers managed detection and response through a specialist partner, and one firm that runs both functions itself. Any of these can succeed. What separates a sound arrangement from a weak one is how it performs against the following considerations.

After-hours coverage. Identify who is watching the environment nights, weekends, and holidays, and how quickly they are expected to act.

Authority to act. Establish who may isolate a system, disable an account, or shut down a connection without waiting for approval, and who must be told when they do.

Internal capacity. Be honest about whether the business has staff who can respond to alerts, coordinate providers, and make decisions under pressure.

Obligations. CMMC, export controls, PCI, and cyber insurance terms can dictate monitoring, log retention, and incident reporting timelines. The arrangement has to satisfy them.

Handoffs. Every additional provider adds a boundary where responsibility can slip. Count the handoffs, and confirm each one is documented.

The emphasis shifts with the type of business. The table below highlights what each member profile should examine closely; it identifies priorities, not a prescribed model.

Evaluation priorities by member profile

Member profile	Where to focus the evaluation
Single-location retailer or range	Who watches the environment after hours, when the business is closed and attacks often begin. Whether endpoint detection and response is included or sold as an add-on. How point-of-sale systems and firearms transaction records are protected and backed up. Cost relative to the size of the environment.
Multi-location retailer, distributor, or e-commerce seller	Consistency of controls across every site. PCI scope and the handling of payment data. Monitoring of the online storefront and cloud accounts. How an incident at one location is contained before it spreads to the others.
Manufacturer supplying the DoD or holding export-controlled data	Whether each provider falls within the scope of the CMMC assessment and can support it. Where CUI, export-controlled data, and security logs are stored and who can reach them. Incident reporting timelines required by contract. Separation of production and shop-floor systems from business IT.

When one firm claims to do both

A growing number of larger providers sell MSP and MSSP services under a single contract. The appeal is genuine: one point of accountability, one onboarding, and security analysts who already know your environment. More mature firms often organize this by splitting the house, with an IT operations team and a separate security team, frequently under different leaders. The split exists because the two functions pursue different missions. IT operations is judged on keeping systems up and users working. Security is judged on reducing risk, which sometimes means taking systems down.

Those missions will collide, and the way a provider resolves the collision reveals more than its service catalog. A security analyst may want to isolate a server on a Friday afternoon while the IT team wants it running through the weekend's busiest sales. Security may flag a misconfiguration that the IT team built. When both teams answer to the same firm, there is a quiet risk that the firm ends up grading its own work, and that findings about its IT team's mistakes are softened before they reach you, or never reach you at all.

Before relying on a combined provider, members should validate the claim rather than accept it on the strength of a sales presentation.

Is the security team real, and is it in-house? Ask whether the security operations center is staffed by the firm's own employees or white-labeled from a third party, how many analysts cover overnight and weekend shifts, and whether the firm holds its own SOC 2 Type II report or ISO 27001 certification. A white-labeled SOC is not disqualifying, but you should know who is actually watching your systems.

How are the two sides separated? Look for distinct leadership and reporting lines for IT and security. Ask whether security findings about the provider's own IT work are reported to you unedited, and request a sample report that shows one.

How are disagreements resolved? Request the written escalation path, confirm who holds final authority during an incident, and ask whether you are told when the two teams disagree about something in your environment. An anonymized example of a real disagreement, and how it ended, is worth more than a policy document.

Can security require IT to act? The security team should have the authority to mandate a fix or halt a risky change, with deadlines, and your contract should reflect that authority rather than leave it to internal goodwill.

Can you separate the services later? Confirm whether you can keep IT services and move security elsewhere, or the reverse, without penalties or loss of your data and logs.

A combined provider that answers these questions clearly can be a sound option for members that value a single accountable partner. One that cannot answer them still has two missions under one roof; the only difference is that the tension between them is hidden from you.

Before bringing on either provider

Several questions apply regardless of which model a member chooses, and they are worth settling before any contract is signed.

Who owns the response? When the MSSP detects ransomware at 2:00 a.m., the contract should state who is authorized to isolate machines, who calls your leadership, and how quickly the MSP must act on the MSSP's findings. If the two providers have never spoken, that conversation should happen before the first incident, not during it.

Where do the providers overlap, and where are the gaps between them? Adding an MSSP, or buying both services from one firm, can create a new version of the same gap this memorandum describes. Each team may assume the other is handling email security, cloud accounts, or vulnerability remediation. A single written responsibility matrix covering both functions prevents that.

What will they need access to? Both providers require privileged access to your environment, and an MSSP typically collects log data that may include sensitive records. Members should know where that data is stored, who can see it, and how long it is retained, particularly where firearms transaction records or export-controlled information are involved.

Does the provider understand your obligations? Ask directly whether the provider supports other firearms industry businesses, federal contractors, or PCI environments, and request references. For manufacturers pursuing CMMC, confirm how the provider fits within your assessment scope before signing, since changing providers mid-assessment is costly.

Who is steering the program? Neither an MSP nor an MSSP sets your security priorities, budgets for them, or reports risk to leadership. Those decisions belong to the business, supported by an internal security lead or a virtual CISO. Without that role, even two capable providers can end up protecting the wrong things well.

Closing the gap

The Quick Guide lays out the work in three stages. Each builds on the one before it, and none requires technical depth from the business owner.

1. Establish the baseline

Start with the core controls in the guide: MFA, endpoint protection, backup and restore, patching, encryption, vulnerability management, logging and monitoring, network segmentation and firewall management, privileged and remote access, and email security. For each, ask two things: is it in scope under our current agreement, and what is its current state? A good MSP will answer both plainly. If the answer to the first is "no," you have found part of the gap, and it belongs in the gap register described at the end of this memorandum.

2. Look at the agreements behind the controls

This stage covers the policies, insurance, and contract terms that govern what happens when something fails. Your security policies and the MSP's should be compared side by side for conflicts. The agreement should state how quickly the MSP will notify you of an incident, and through whom. You should know where your cyber insurance ends and the MSP's liability begins, and whether the MSP's own coverage is large enough to absorb losses its negligence might cause. Subcontractors and third-party tools that touch your data warrant written disclosure. Exit terms, SLAs, data portability, and license ownership belong on the table now, while the relationship is healthy, rather than in the middle of a dispute.

3. Verify on a schedule

Assurances fade and environments change, so verification needs a calendar. At minimum, that means an annual report of the MSP's security controls measured against a recognized framework, routine artifacts showing patching and backup testing, and a yearly full restore test that records actual recovery time and data loss against what the business can tolerate. Policies and practices deserve a fresh look whenever the business changes shape, whether through a new location, a new contract, or a new system.

The table that follows contrasts common assurances with the evidence that should stand behind them.

Area	What the MSP will usually say	What to ask to see
Backups	"Backups are completing successfully."	Results of a full restore test, with the actual time it took (RTO) and how much data was lost (RPO).
Patching	"We patch monthly."	A patch compliance report for every endpoint and server, including exceptions and why they exist.
MFA	"MFA is turned on."	Which systems it covers. Email alone is not enough; remote access, admin accounts, and cloud consoles need it too.

Area	What the MSP will usually say	What to ask to see
Privileged access	"Only our techs have admin."	A current list of every account with admin rights, including the MSP's own shared or tool accounts.
Incident response	"We'll handle it."	A written plan naming who calls whom, how fast you are notified, and who decides on containment.
Insurance	"We're insured."	A certificate showing cyber and errors-and-omissions limits, and whether it covers losses to clients.
Subcontractors and tools	Often not raised at all.	A list of third parties and platforms (RMM, PSA, backup, AI tools) that can reach your systems or data.
Exit terms	"It's in the contract."	Termination fees, data return format and timeline, license transfer, and offboarding obligations, in writing.

Questions about the MSP itself

The final section of the Quick Guide turns to the provider as a business. What is the MSP's own continuity plan if it suffers a breach or an outage? If its tools are compromised, how will it contain the damage and communicate with clients? Does it offer mobile device management and phishing awareness training, or will you need to source those elsewhere? And is it keeping current with the vendors and practices it relies on?

Raising these questions with a provider you trust can feel awkward. Capable MSPs tend to welcome the scrutiny, since clients who understand the scope of the relationship are easier to serve and far less likely to be blindsided. Resistance tells you something as well.

A practical starting point

For a business examining its MSP relationship this way for the first time, the first month should produce five things:

- A marked-up copy of the current MSP agreement showing what is explicitly in scope for security.
- A working session with the MSP covering each baseline control in the Quick Guide, with current state and supporting evidence.
- Written confirmation from your cyber insurance broker of what the policy requires of you and your providers, including any mandated incident response firm or MFA conditions.
- Results from a restore test of one critical system, including how long recovery took.
- A short gap register recording, for each finding, whether the business will close it, transfer it, or formally accept it.

The register is the piece most businesses skip, and it does the most work. Some risk will remain after every gap is reviewed. The difference is that leadership chose it with open eyes, on a calm afternoon, rather than learning about it from a ransom note.

About Fellsway

Fellsway is a Greater Boston–based Cyber & AI Readiness Advisory firm and NSSF Industry Association partner that helps firearms manufacturers, distributors, and retailers stay secure, compliant, and resilient. From CMMC readiness for defense suppliers to vCISO leadership, incident response planning, and executive tabletop exercises, Fellsway protects the data, contracts, and operations that firearms businesses depend on.

For more information or to get in touch, visit www.fellswaygroup.com.

About NSSF Project Cybersafe

The firearm industry faces a range of emerging cyber threats that pose significant risks to manufacturers, retailers, ranges and consumers alike. To combat these challenges, NSSF's Project CyberSafe initiative is dedicated to helping firearm industry businesses and their employees stay informed and proactive, thereby enhancing their defenses against these evolving threats

For more information on this and other topics, visit www.projectcybersafe.com.