GATE 15

ANALYSIS ▪ RESILIENCE ▪ OPERATIONS

15 from 15

Cybersecurity Mitigation & Resilience Fundamentals

Understand the Threats.
Assess the Risks.
Take Action.

September 2026

Blocking and Tackling

Introduction by Andy Jabbour, Founder & CEO, Gate 15

When I played high school football, I was a lineman. I played both the offensive and defensive lines, and much of the job came down to the fundamentals of blocking and tackling. The ideas are not complicated. Executing them consistently under pressure, against someone determined to beat you, is much more difficult. For all the excitement of the game, the teams that are best at the fundamentals usually give themselves the best chance to win.

Why 15 from 15?

The 15 from 15 framework outlines key actions but is not exhaustive and is not a substitute for comprehensive cybersecurity programs or frameworks. These areas aim to improve security, readiness, and resilience at individual, team, operational, executive, and board levels. Most importantly, they are easy to implement..

The criticality of fundamentals was reinforced as I competed in powerlifting and served in the Army, and it has only been further underscored by everything I have done over the last twenty years. This focus still shapes how I think about security and resilience today. Gate 15 is a blocking-and-tackling company. We spend every day studying evolving cyber threats, ransomware and extortion, artificial intelligence, exploited vulnerabilities, insider risks, supply chain compromises, operational technology concerns, geopolitical tensions, and other threats and risks across the global cyber and all-hazards space. We report on these every day and discuss these issues every week across our podcasts, delivering threat-informed analysis to our supported clients and communities. We also see an endless stream of new technologies and products promising to solve the latest problem. Some are excellent; some are... not excellent. None eliminate the need to execute the fundamentals.

For years, Gate 15 has helped organizations understand threats, assess risk and readiness, develop practical plans, exercise capabilities, and learn from real events. Our team led the development and subsequent refresh of WaterISAC's Cybersecurity Fundamentals for Water and Wastewater Utilities. That work reinforced a lesson that extends far beyond the Water and Wastewater Systems Sector: even as the threat environment evolves, many of the most important actions organizations can take remain remarkably durable.

Earlier this year, I took this message on the road. At the TribalHub Cybersecurity Summit in Jacksonville, Florida, I led a full session on why and how organizations can build their own cyber tabletop exercises. I then continued the conversation across the country while supporting TribalHub's regional conferences. In discussions with Tribal technology and security leaders, the message was the same as what we share with critical infrastructure organizations, businesses, nonprofits, faith-based organizations, and other communities: understand the threats, but do not become overwhelmed by them. Focus on risk. Focus on impact. Focus on practical mitigation and resilience.

That is the purpose of 15 from 15. These are not the only actions an organization should take, nor are they a substitute for a mature cybersecurity program or established frameworks. They are fifteen practical areas that consistently improve security, preparedness, and resilience. They apply at the individual, security-team, operational, executive, and board levels. Most importantly, they are actionable.

This is not complicated, but it is not easy. Fundamentals require discipline, repetition, investment, leadership, and a willingness to keep learning. That is the blocking and tackling.

Cyber and all-hazards risk and resilience. At Gate 15, we apply a threat-informed & risk-based approach to analysis, resilience, & operations, helping to secure America's **People, Places, Data, & Dollars.**

15 from 15: Mitigation & Resilience

If you read nothing else in this paper, start here. Review these fifteen areas honestly. Identify where your organization is strong, where it is weak, and where a practical improvement could meaningfully reduce risk. Then act. Then keep going. You do not need to become championship-caliber in every area tomorrow. Break the work into manageable pieces, set priorities, establish near- and longer-term goals, and get a little better every day. The objective is deliberate progress toward the level of maturity your mission and risk require.

Task	Action
Assess	Know where you are so you can build a realistic path to where you want to be.
People	Make security everybody's business, from every user to the CEO.
Organizational Culture	Make security, safety, and resilience part of how the organization operates.
Security Stack	Build layered, best-practice security capabilities - and actually operate what you buy.
Information Sharing	Join trusted communities, participate, contribute, and learn from your peers.
Multi-Factor Authentication (MFA)	MFA all the things, then keep moving toward stronger, phishing-resistant methods.
Network Segmentation	Separate what should not talk, control what must, and build an architecture you can support.
Patching	Know it, prioritize it, patch it - or mitigate it - at the speed of risk.
Backups & Encryption	Protect your data and ensure you can recover your business.
Planning	Build executable plans before the crisis and keep them up to date.
Out-of-Band (OOB) Communications	Know where to communicate when normal communications are unavailable or untrusted.
Train	Plans and tools do not execute themselves. Train the people.
Test	Validate that systems, controls, procedures, and capabilities actually work.
Exercise	Put the team on the field and practice before game day.
Post-Mortems	Learn from everything, document it, improve, and do it again.

The 15 are interconnected, neither fully sequential nor independent. Assessment establishes the baseline and priorities; people and culture turn expectations into behavior; information sharing provides threat context, peer experience, trusted relationships, and practical solutions; technology and controls reduce exposure; planning, training, testing, and exercises build readiness; and post-

mortems feed lessons back into plans, priorities, and the next assessment. Strong organizations use the fundamentals together. Start where you are, decide where you need to go, and turn the journey into manageable bites you can resource, execute, measure, and improve.

> This is resilience: Doing the work up front to prepare for a disruption, anticipating that it will in fact happen, and exercising not just for response but with a deliberate focus on continuity and recovery, improving the ability to operate in a degraded state and significantly reducing downtime when an incident occurs.
>
> *~ Former CISA Director Jen Easterly, 09 Aug 2023, "The Power of Resilience"*

1. Assess

What it is. You have to know where you are before you can figure out how to get where you want to go. A cybersecurity assessment provides that baseline. It should help the organization understand relevant threats; critical People, Places, Data, and Dollars; technology; dependencies; controls; plans; maturity; and the consequences of disruption. That starts with knowing what is actually in your environment. In an August 2026 alert responding to increased targeting of operational technology, the UK's National Cyber Security Centre (NCSC) warned organizations not to assume systems are inaccessible from the internet without verification, noting that misconfigurations, legacy connections, and unmanaged assets can create unintended exposure. **Know what you have. Know what is exposed. Know how it connects.** The goal is not to chase a perfect score. It is to establish an honest current state, identify a realistic target state, and determine the priorities that move you from one to the other.

What to do. Start somewhere. Organizations can self-assess using the National Institute of Standards and Technology Cybersecurity Framework 2.0 (NIST CSF 2.0), the Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Performance Goals, sector guidance, or another appropriate framework. Review more than technical controls. Plans, policies, procedures, prior assessments, after-action reports, incident reports, post-mortems, vendor relationships, insurance requirements, and public or contractual commitments help show what the organization says it does and where reality may differ. Interviews with security, information technology (IT), department leaders, operations, and executives help complete the picture. Then prioritize. Some improvements may be immediate and inexpensive; others may require a multi-year roadmap, staffing, capital investment, or leadership decisions.

Why it matters. An assessment turns uncertainty into a plan of action. When Gate 15 conducts an assessment, we combine established frameworks with our threat-informed, risk-based perspective and the 15 from 15 fundamentals. We use a third-party cloud-based assessment platform to organize and analyze assessment information. The platform supports the process but does not replace practitioner judgment. We identify gaps, validate them with the organization, and senior Gate 15 leadership reviews the findings and practical recommendations. The value is not the score or report. The value is the roadmap: where are we today, where do we want to be, what matters most, and what should we do next?

2. People

What it is. Security does not belong to IT, the help desk, the CISO, the CIO, or the security team. Those teams may lead and enable security, but security is everybody's business. Ultimately, accountability rests with the CEO or organizational leader. Everyone can help protect the organization, and everyone can also become an entry point for an adversary.

What to do. Make the entire team security-minded. Set expectations, provide ongoing education, remind people what suspicious behavior looks like, and make it easy to report concerns and mistakes quickly. Personnel should pause and think before clicking a link, sharing sensitive information, approving an unexpected MFA prompt, or acting on an unusual request. Security, IT, operations, legal, communications, finance, HR, physical security, and leadership should understand their roles before an event. Build people up and support them while holding them to reasonable standards and accountability.

Why it matters. People are not merely vulnerabilities to manage. Properly informed personnel are human sensors distributed across the organization. They can recognize phishing, question unusual financial requests, identify suspicious physical activity, or report a technology issue before it becomes a crisis. And a championship football organization is not just the Pro Bowlers or the 53 players on the roster. It is the coaches and front office, trainers and medical staff, equipment and sideline personnel, analysts, and everyone else doing their jobs so the team can win. Security and resilience work the same way. Prepared people recognize problems earlier, make better decisions, coordinate faster, and support one another. Get everybody on the security team.

3. Organizational Culture

What it is. People establish individual responsibility. Culture determines whether the organization collectively believes, reinforces, and lives that responsibility. Security and resilience should not be things the organization does only occasionally; they should become part of how the organization operates and who it is.

What to do. Build a culture where everyone - from those touching computers, switches, routers, operational systems, facilities, financial processes, and customer or community services to personnel in every department and executive leadership - understands that security, safety, and resilience support the mission. Leaders need to sing from the same songbook and demonstrate through decisions, budgets, time, recognition, and accountability that the responsibility is real. Security is not important for security's sake; it helps the organization serve its community, protect people and assets, remain profitable where appropriate, and continue operating through adversity. Encourage people to keep their heads on a swivel, report concerns early, and take pride in protecting the team. A security-minded culture understands not only the importance of protecting our People, Places, Data, and Dollars, but also that leaders care about that responsibility and are invested in it.

Why it matters. A resilient culture is especially visible when things go wrong, but it is built through the decisions made before anything goes wrong. Organizations should not discover collaboration for the first time during a ransomware attack, severe weather, a hostile event, an infrastructure outage, or another disruption. Trust, communication, shared responsibility, and disciplined habits should already be in place. Just as importantly, awareness has to lead somewhere. In its 2026 Cyber Series

discussion on Institutional Willful Blindness, the UK's National Cyber Security Center (NCSC) examines why organizations can understand cyber risk yet still fail to act, emphasizing how leadership behavior, organizational culture, communication, and risk framing can create a gap between knowing and doing. Gate 15 discussed the same challenge in Weekly Security Sprint EP 172: security information can be uncomfortable and inconvenient, but resilient leaders do not bury it or respond reflexively. They engage it, seek to understand the root cause and operational context, weigh likelihood and consequence, determine what can reasonably be mitigated, explicitly accept residual risk where appropriate, and support the business in operating as securely as possible. Leaders should challenge themselves: how am I receiving uncomfortable risk information? Am I enabling thoughtful action, or am I becoming an obstacle? Fundamentals become powerful when they stop feeling like special activities and become simply how we do things here.

4. Security Stack

What it is. Build the best security stack your organization can reasonably support. That does not mean buying every shiny new product. It means using layered, established security capabilities that align with your risks, your industry, and your ability to operate them.

What to do. Benchmark. Talk to peers and your Information Sharing and Analysis Center (ISAC). Ask what comparable organizations use and what works. Talk to your cyber insurer or broker about recommended controls, preferred providers, available discounts, and whether stronger controls can improve your insurance profile. Cover the basics well: endpoint protection, secure email, firewalls, logging and monitoring, identity controls, secure remote access, vulnerability management, backups, MFA, and the environments that matter to you - including cloud, mobile, operational technology (OT), Internet of Things (IoT)/Industrial Internet of Things (IIoT), and building systems. CISA's current logging guidance emphasizes enabling useful logs across servers, firewalls, endpoints, cloud services, and other systems; centralizing them where practical; protecting them from unauthorized access or deletion; establishing alerts for high-risk activity; and ensuring that trained personnel actually review them. If the ideal stack is beyond today's budget or staffing, implement the highest-value capabilities now and put the rest on a deliberate roadmap.

Why it matters. You do not necessarily have to be the fastest gazelle on the savanna, but you do not want to be the easiest one for the lion to catch. Attackers often choose the easier path. But owning security technology is different from having security capability. Gate 15 saw security technology correctly generate a warning that went unnoticed because no one was monitoring it; a manageable cyber event became more consequential than it needed to be. Configure the tools. Monitor them. Maintain them. Train people to use them. Know who acts when an alert fires. Technology should reduce risk; not simply create another dashboard nobody is watching.

5. Information Sharing

What it is. No organization sees the entire threat environment on its own. Trusted information-sharing communities provide warnings, peer lessons, indicators, mitigations, relationships, and a sounding board for questions ranging from “Is anyone else seeing these IOCs?” to “What technology are you using?” to “Can I see how you structured your incident response plan?”

What to do. Join your sector, subsector, or community ISAC or ISAO - and consider more than one community when your mission crosses sectors. Build local relationships through InfraGard, fusion centers, law enforcement, emergency management, and trusted peers. Use trusted threat intelligence platforms and services, such as Gate 15's GRIP, to stay regularly informed. Then participate. Join working groups. Ask questions. Answer questions. Share in collaboration spaces. Designate an information-sharing champion and an alternate, and contribute to collective awareness. Work with legal and leadership before an incident to define what you can share, with whom, and under what conditions.

Why it matters. Do not let organizational resilience depend entirely on one person's private relationships, and do not just lurk. Institutionalize the relationships and contribute to them. Your ISAC can provide sector- and global-threat context, peer experience, practical mitigation ideas, trusted vendor feedback, and relationships you may need during a crisis; local communities can provide regional context and connections. In a recent Gate 15 Interview recorded with Potawatomi Casino Hotel IT Director Adam Gruszczynski, Adam described discovering a serious vulnerability in the hotel's door-locking technology shortly before Milwaukee hosted the Republican National Convention. Vendor support was not providing an answer. He reached out to the Tribal-ISAC community, received useful peer guidance within hours, and the team addressed the vulnerability before it became an incident. That is information sharing in practice: cyber risk, physical consequences, trusted peers, and action. Join your ISAC, get involved, and contribute.

6. Multi-Factor Authentication (MFA)

What it is. MFA is no longer an advanced security control. It is a foundational baseline. Microsoft Research found that MFA reduced the account-compromise risk by 99.22% across the studied population and by 98.56% even among accounts with leaked credentials. Few cybersecurity actions offer that kind of risk reduction for the relative cost and implementation complexity.

What to do. MFA for all the things. Require it wherever technically feasible, prioritizing privileged accounts, email, remote access, cloud services, financial systems, and other high-value applications. Encourage personnel to use MFA on personal email, financial accounts, and social media too. Some MFA is better than none, but stronger MFA is better than weaker MFA. Move from SMS or basic one-time codes toward authenticator-based methods and, where feasible, phishing-resistant options such as passkeys or security keys. If today's solution is the best you can support, use it now and put stronger authentication on the roadmap.

Why it matters. Technology alone is not enough. Train personnel to recognize MFA fatigue or prompt bombing. Stop. Did I initiate this login? Does the timing and location make sense? If not, do not approve it and report it. The threat remains immediate: in September 2026, the Australian Signals Directorate (ASD) reported that 42% of incidents involving industry, government, and critical infrastructure reported to ASD in 2024-2025 involved compromised accounts or credentials. ASD's Australian Cyber Security Centre (ACSC) emphasized that passwords alone are no longer enough and encouraged phishing-resistant MFA such as passkeys, with authenticator applications where passkeys are not supported. As one of cybersecurity's most established and effective fundamental controls, failing to implement MFA where it is readily available is not merely a technical deficiency; it is a leadership-level risk that should require explicit justification and ownership.

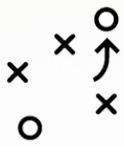
7. Network Segmentation

What it is. The concept is easy: isolate systems and functions so one compromise does not become every compromise. Separate IT from OT. Separate guest, vendor, administrative, building, development, and other environments where risk warrants it. Protect the crown jewels and control the pathways that genuinely need to remain open.

What to do. The hard part is operational reality. Every additional segment creates something that must be configured, patched, monitored, documented, and understood. Gate 15 has seen organizations with segmented environments still suffer significant consequences because less-attended systems within those environments were not maintained. Segmentation without maintenance can create false confidence. Use firewalls, VLANs, DMZs, jump hosts, access controls, and stronger isolation technologies where appropriate, but build an architecture your team can actually support.

Why it matters. Separate what does not need to be talked about. Control what does. Default-deny where practical. Pay particular attention to IT-to-OT, remote-access, third-party, and building-system pathways. NCSC's August 2026 warning on disruptive cyber activity specifically calls for separating management networks, OT control systems, and business IT networks based on function and criticality, while restricting communications between zones to those required for operations. The objective is straightforward: prevent unauthorized access, make adversary movement more difficult, and reduce the likelihood that compromise in one environment becomes compromise everywhere. If the ideal architecture is beyond today's resources, document the desired state, prioritize the highest-risk separations now, and deliberately build toward the target. **Your network segmentation has to be supportable, or you are setting yourself up for failure.**

8. Patching



What it is. Patching sounds simple: keep systems up to date. The real discipline is vulnerability management - knowing what is in the environment, knowing what needs attention, understanding what matters most, knowing who decides, and moving at the speed of risk.

What to do. Maintain current asset visibility, clear ownership, vendor and government notifications, routine patch cycles, and an out-of-band process for urgent issues. CISA's Known Exploited Vulnerabilities Catalog should be a standing input: if a vulnerability in your environment is in KEV, adversaries are already exploiting it in the wild. Your ISAC can add sector context - what peers are seeing, what is being exploited now, and where others are prioritizing action. When immediate patching is unsafe or impossible, especially in OT or legacy environments, apply compensating controls such as segmentation, access restrictions, monitoring, or isolation and document the residual risk.

Why it matters. The risk calculation changes. Roughly a decade ago, while visiting several global, high-profile organizations in New York City, Gate 15 leadership had candid conversations with security leaders about patching during their most consequential operating periods. At the time, some described windows lasting weeks or months when they believed the operational risk of a failed patch outweighed the cyber risk of temporarily carrying a vulnerability. Those were sophisticated

organizations making deliberate risk decisions based on the day's environment. We know that they would not make the same calculation the same way today. Exploitation moves faster, internet exposure is broader, dependencies are more complex, and CISA's Known Exploited Vulnerabilities (KEV) Catalog provides defenders a clear signal when adversaries are already exploiting a flaw. Artificial intelligence (AI) is further compressing the timeline as vulnerability discovery accelerates and adversaries improve their ability to operationalize findings. Leadership needs to understand what prevents the organization from moving faster - people, technology, process, or budget - and make the risk-versus-reward decision. Know it. Prioritize it. Patch it - or mitigate it - and keep getting faster.

9. Backups & Encryption

What it is. Assume prevention will eventually fail. Backups preserve the information and configurations needed to restore operations; encryption protects sensitive information when an adversary gains access. Together they reduce consequences and support resilience.

What to do. Start with tried-and-true practices such as the 3-2-1 backup rule, adapted as appropriate for your environment. Back up critical data, system images, configurations, cloud information, and OT/industrial configurations. Protect copies from the production environment and increasingly consider immutable backups. Test restoration - a backup you have never successfully restored is a hope, not a recovery capability. NCSC's current OT guidance similarly emphasizes tested backups and recovery procedures, including critical configurations, controller logic, and engineering data, and recommends designing backups to withstand ransomware attacks. Just as importantly, organizations should regularly practice restoration and recovery rather than assuming that having a backup means they can recover. Consider geography and common dependencies too. Severe weather, flooding, wildfire, power or telecommunications outages, physical attacks, hostile events, active-shooter incidents, cloud failures, and cyberattacks can all affect access to both primary and backup environments. Ask what could take out both. Encrypt sensitive information at rest and in transit, and protect the keys.

Why it matters. Ransomware and destructive attacks become far more consequential when recovery is uncertain. Proper encryption can also dramatically reduce the usefulness of stolen PII, PHI, financial data, intellectual property, and sensitive employee information when attackers cannot obtain the keys. Recent industry research illustrates the gap between backup confidence and actual resilience. Recent research by Omdia found that 93% of surveyed technology leaders considered absolutely immutable backup storage critical to ransomware protection, while only 16% said their current backup environment met that standard[1]. The broader resilience lesson is consistent with government guidance and incident experience: having backups is different from being able to recover. Organizations should independently validate immutability, restoration performance, recovery objectives, and the procedures for restoring essential operations. Talk to your ISAC, peers, and insurer about proven technologies and expectations. Strong investments in backup and encryption may be expensive, but the business case becomes clearer when leadership compares the cost of resilience against downtime, recovery costs, lost revenue, legal expenses, and reputational harm.

[1] A backup-storage vendor commissioned this research and the findings should be considered in that commercial context.

10. Planning

What it is. You cannot improvise your way through a crisis. Build the plays before you need to run them. But do not wait for the perfect plan either. Start with something reasonable and executable, then keep improving it.

What to do. Begin with a cyber incident response plan. If necessary, use a credible government, ISAC, or peer template as the starting point. Then mature toward scenario-specific runbooks and playbooks, crisis management, crisis communications, business continuity, disaster recovery, ransomware response, and other plans appropriate to your organization. Prioritize the most likely and most consequential threats first. Define roles, authorities, escalation thresholds, decision points, notification procedures, dependencies, contacts, and alternates. Know when a technical incident becomes a corporate crisis and how that transition occurs. Build cyber-insurance contacts, requirements, approved vendors, and coverage considerations into the process.

Make plans executable, not novels. Reality will not follow the script exactly, so the plan needs to provide enough structure to pivot intelligently when the play changes. Store plans so they remain available when primary systems are unavailable, including controlled hard copies or, where appropriate, protected alternate access. Define when plans are reviewed and updated - on a regular cadence and after incidents, exercises, major organizational or technology changes, and other meaningful triggers. Also ask what the organization has already promised. ESG statements, SEC filings, insurance applications, contracts, regulatory submissions, and public statements may commit the organization to plans, controls, training, or exercises. Know what you have promised and make sure you can prove you are doing it.

Why it matters. You do not walk onto a football field against a well-trained, well-coached opponent and wing it. You have a playbook. You know your assignments and options. You practice the plays. Planning reduces improvisation on the worst day, exposes gaps before an incident, and aligns technical, operational, and executive teams. Gate 15 can help organizations build, refine, and connect these plans. Whether you do it internally or with outside support, have the plans in place and keep improving them.

11. Out-of-Band Communications

What it is. If your primary communications environment becomes unavailable or untrusted, everyone should already know where to go next. During a ransomware attack or another compromise, continuing to discuss the response on systems that an adversary may be monitoring is a bad plan. Severe weather, power and telecommunications outages, physical attacks, hostile events, cloud failures, and other all-hazards disruptions can create the same need.

What to do. Identify the approved alternate platform or method before the crisis. It may be another enterprise platform, Signal, WhatsApp, alternate email, phones, radios, or another solution appropriate to your risk. Avoid recreating all the same dependencies as the primary environment. The 2019 Baltimore ransomware attack provides a useful illustration: City systems were disrupted, email communications were limited, desktops were frozen, and departments created workarounds using cell phones, laptops, new platforms, phone calls, and even pen and paper while recovery

continued. Do not design the alternate after the primary system fails. Document the switchover criteria: who makes the call, how people know the switch occurred, where they go, and who administers the alternate environment. Pre-enroll users, establish role-based continuity where appropriate, maintain contact information, and identify alternates. Then train and practice. A simple quarterly communications drill can reveal expired accounts, changed phone numbers, forgotten passwords, and missing personnel before a real event does. Critical infrastructure organizations should also consider resilient communications programs, such as the Government Emergency Telecommunications Service (GETS) and, where eligible, the Wireless Priority Service (WPS), and practice making the GETS call. InfraGard relationships can help eligible members understand and request these capabilities.

Why it matters. The middle of a ransomware attack is a terrible time to start exchanging personal email addresses. OOB communications are low-hanging fruit: identify them, document them, train on them, exercise them, and maintain them. Do not assume that because the backup channel exists, it will work when you need it.

12. Train

What it is. You can have the plans, the tools, and the technology. The next question is simple: who knows how to use them? Training provides people with the knowledge and skills to recognize threats, apply controls correctly, and fulfill assigned responsibilities.

What to do. Training is not a one-and-done onboarding requirement, an annual refresher, or Cybersecurity Awareness Month. Those are useful pieces, but readiness requires repetition. Provide recurring security awareness and role-specific training. Accounts-payable employees, network administrators, executives, communications leads, and operators do not need identical training. Use current incidents and ISAC reporting to make training relevant. If your sector is experiencing a particular phishing campaign today, tell your people today. And give personnel time to train. In The Gate 15 Interview with Adam Gruszczynski, he highlighted a challenge familiar to many lean teams: sending someone to two days of training also means two days of work that still needs covering. Leadership has to recognize that tension and deliberately invest the time, not just the tuition. Competence is an organizational expectation, and developing it requires organizational support.

Why it matters. You do not go to the gym once and get stronger. You train, recover, come back, increase the load, and repeat. The same applies here. Training is also not exercising. Build the plan, train the people, test the capabilities, and then exercise the organization. The exercise should not be the first time participants see the plan or learn their responsibilities. Plans do not execute themselves. Technology does not operate itself. To get stronger, to build muscle memory, to execute properly, you have to put in the reps. Do the work.

13. Test

What it is. Testing asks a straightforward question: does this thing actually work the way we think it works? Testing is not exercising. Organizations need both.

What to do. Penetration testing is the clearest example: have qualified personnel attempt to defeat defenses and identify weaknesses before an adversary does.

Testing can also include vulnerability scanning, phishing simulations, backup restoration, failover testing, access-control validation, segmentation validation, alert testing, disaster-recovery testing, and OOB communications checks. Testing may be internal, external, government-supported, or performed by trusted service providers. Talk to your ISAC about reputable providers and peer experience. Talk to your insurer about expectations, preferred providers, potential discounts, and appropriate frequency. Test what matters most to your risk, track findings to closure, and retest important fixes.

Why it matters. Training asks whether people know what they are supposed to do. Testing asks whether the system, control, procedure, or individual capability works. Exercising asks whether the organization can bring people, plans, processes, technology, and decisions together under realistic conditions. Plan it. Train it. Test it. Then exercise it. And if testing finds a weakness, fix it - otherwise you have simply paid someone to document a problem you still have.

Understand the Threats. Assess the Risks. Take Action.

Over the past two years, our company has implemented several technology and security enhancements and has worked closely with Gate 15 to conduct a series of executive-level exercises, a post-mortem of a cyber event, and a cybersecurity assessment. Through these initiatives, we achieved a 34% reduction in our cyber insurance costs.

~ Director, Cybersecurity & Infrastructure for a leading U.S. solar and energy manufacturer.

14. Exercise

What it is. Exercises put the team on the field before game day. They allow organizations to practice plans, decisions, coordination, communications, continuity, and recovery in a controlled environment. Gate 15 follows FEMA's Homeland Security Exercise and Evaluation Program, HSEEP, a tried-and-true methodology used from local responders through complex national-level exercises. HSEEP provides the structure; experience teaches how to make an exercise work in the room.

What to do. Start somewhere, even if the budget is zero. Designate an exercise champion. Use HSEEP and CISA exercise resources. Ask your ISAC about scenarios, grants, peer activities, and opportunities to participate. Talk to government partners. Then choose the right activity. A workshop is useful when you are building a policy, plan, procedure, or other product. A tabletop exercise uses a scenario and structured discussion to determine whether plans, roles, decisions, and assumptions make sense. A drill validates a specific operation or capability, such as switching to OOB communications. A functional exercise increases complexity and can bring together security, executives, communications, legal, insurance, vendors, MSSPs, public-sector partners, and other stakeholders. Full-scale exercises can add real personnel and field activity and may be especially valuable for active-shooter, mass-casualty, physical-security, and other all-hazards scenarios.

Build progressively. Gate 15 generally encourages at least one cybersecurity-focused executive exercise annually, at least two security team exercises annually, and more frequent drills, potentially quarterly, depending on risk and resources. A firm but flexible multi-year training and exercise plan can deliberately move an organization from its current capability to its target state. Exercise the most likely and most consequential scenarios. Focus on decisions, not merely actions: who has authority, when leadership engages, how information flows, what tradeoffs exist, when alternate communications begin, what insurance requires, how continuity works, and what success looks like. Bring the right people to the table. Board members, executives, legal, insurance/risk, communications, operations, security, IT, departments, service providers, vendors, and public-sector partners all see different pieces of the problem.

Why it matters. The need is real. Some industry reports suggest that only about one-third of organizations have conducted tabletop exercises[2]. More recently, Tribal-ISAC's 2025 Tribal Cybersecurity Survey, published in The Pulse, found that only 44% of responding Tribal organizations had conducted tabletop exercises. Encouragingly, Adam Gruszczynski noted in The Gate 15 Interview that the forthcoming 2026 Pulse data show year-over-year improvement in Tribal exercise participation. Progress is happening, but the gap remains significant. Exercises expose assumptions, clarify decisions, build relationships, and create business cases before the crisis. Gate 15 has seen executive exercises turn an abstract resilience gap into a clear investment decision, as leadership could finally see the risks, costs, and consequences of doing nothing. You can do exercises yourself, and we encourage you to start. Tribal-ISAC's member tabletop exercise grant is one example of how a trusted community can help remove cost and resource barriers. If you want an experienced outside team to design realistic scenarios, facilitate difficult conversations, challenge assumptions, and turn the results into improvement, this is what Gate 15 does.

15. Post-Mortems

What it is. Learn from everything. A post-mortem is a structured opportunity to understand what happened, what worked, what did not, and what should change. It does not require a crisis-level event. Major incidents, smaller cyber events, near misses, drills, tests, and exercises can all provide valuable lessons.

What to do. The exercise may be the fun part, but the value is not complete until the after-action report and improvement plan are finished. Capture strengths and areas for improvement. Identify what will change, who owns the action, the expected timeline, and how completion will be tracked. After a smaller event, the review may simply be an hour with the security team. After an enterprise crisis, the process may include executives, legal, communications, operations, insurance, vendors, and other stakeholders. Scale the review to the event; keep it focused on learning rather than blame, and follow the lesson wherever it leads - plans, training, technology, staffing, procedures, insurance, testing, or another exercise.

Why it matters. Lessons identified are not lessons learned until something changes. Gate 15 has conducted post-mortems after major incidents and after smaller cyber events where leadership simply wanted an independent perspective on what happened and how to improve. That is a healthy

[2] JumpCloud, "Incident Response Statistics to Know in 2025," 8 January 2025. JumpCloud reports that only 35% of businesses run cybersecurity tabletop exercises and attributes the statistic to CISA; Gate 15 treats this as secondary industry reporting.

security culture: pause, learn, document, improve. Then feed the lessons back into plans, training, testing, exercises, and the next assessment. Football teams watch film after the game. They study the blown assignment and the plays that worked, adjust, practice, and get better. Learn during the regular season. Improve for the playoffs. Bring your best game when the championship is on the line.

Fundamentals Build Resilience

The concepts in 15 from 15 are simple. Being excellent at them is harder. Blocking and tackling work only when you practice, reinforce, and execute them consistently. Cybersecurity and organizational resilience are the same.

The objective is not to eliminate every risk. That is impossible. The objective is to reduce the likelihood of disruption, reduce the consequences when preventive controls fail, protect **People, Places, Data, and Dollars**, sustain essential operations, make better decisions under pressure, and recover as quickly and safely as possible.

Protect Our Nations
People, Places, Data, and Dollars

The goal is not to eliminate all risks, which is impossible. Instead, it aims to reduce the chances, minimize impact when controls fail, protect People, Places, Data, and Dollars, maintain operations, make better decisions under pressure, and recover quickly and safely.

Preparedness is a marathon, not a sprint. Resilience is built through a continuous cycle. Assess where you are. Understand the threats. Build the people, culture, technology, relationships, controls, and plans. Train. Test. Exercise. Learn. Improve. Reassess. Nothing is one-and-done, and very few organizations can do everything at once. Set priorities, make the work achievable, celebrate progress, and keep moving toward the level of readiness your mission requires. Recent NCSC guidance makes the same point in responding to today's disruptive cyber activity: long-term resilience requires organizations to prepare before an incident and to establish, maintain, and regularly exercise their ability to respond and recover.

You can do much of this yourself. Use NIST, CISA, FBI, FEMA, ASD/ACSC, NCSC UK, the Canadian Centre for Cyber Security, your sector guidance, and your trusted partners. Join your ISAC. Join the GRIP. Learn from your peers. And when you need additional capacity, perspective, or an experienced partner, Gate 15 can help with threat intelligence, cyber assessments, planning, workshops and exercises, and post-mortems.

We do not just tell organizations what could go wrong. We help them practice what happens next.

About Gate 15

Gate 15 provides a range of services to help organizations prepare for, recover from, and defend against cyber disruptions. The services outlined can be useful on their own but are even better as part of a continuous preparedness strategy.

- **Understand the Threats with the GRIP.** Resilience begins with a collective understanding of the threats and their potential operational impacts. The GRIP delivers a daily bulletin with timely, actionable information to the people who need to assess risk to their organizations.
  Join the GRIP!
- **Evaluate Risks with Cyber Assessments.** Equipped with a daily feed of pertinent threat information from the GRIP, leaders can assess their risk through the Cyber Assessment. Gate 15 will help uncover weaknesses and evaluate potential impacts on business operations. Gate 15 will translate findings into prioritized recommendations to help leadership make informed decisions.
- **Develop Plans That Turn Awareness into Action.** Assessments tell a story about risk, but to mitigate the risk, priorities must be translated into implementable plans. Gate 15 can create customized incident response, continuity, and recovery plans tailored to each organization, detailing roles, decision-making authority, communication protocols, escalation procedures, and response steps in advance of a disruption.
- **Validate Readiness Through Exercises.** A plan is only valuable when it can be validated in practice. By collaborating with Gate 15, leadership can design realistic exercises that present credible scenarios and challenge decision-making, coordination, communication protocols, and response strategies. An exercise evaluates organizational performance under pressure while uncovering hidden gaps in a controlled setting.
- **Learn and Improve Through Post-Mortems.** When a real-life incident occurs, Gate 15 can work with your organization to conduct a structured review to determine what happened, why it happened, what worked, what did not, and what should be improved.

Understand the Threats. Assess the Risks. Take Action.

Cyber and all-hazards risk and resilience.

At Gate 15 we apply a **threat-informed** & **risk-based** approach to **analysis, resilience, & operations**, helping to secure America's **People**, **Places**, **Data**, & **Dollars**.

Learn more at www.gate15.global. Join **Gate 15's Resilience and Intelligence Portal** (GRIP) and connect to our homeland security community. **Join the GRIP!**

Selected References & Resources

- **National Institute of Standards and Technology.** *The NIST Cybersecurity Framework (CSF) 2.0*. 26 Feb 2024.
- **Cybersecurity and Infrastructure Security Agency.** *Cross-Sector Cybersecurity Performance Goals*.
- **Cybersecurity and Infrastructure Security Agency.** *Known Exploited Vulnerabilities Catalog*.
- **Federal Bureau of Investigation.** *Operation Winter SHIELD: Ten Actions to Improve Cyber Resiliency*. 2026.
- **Federal Emergency Management Agency.** *Homeland Security Exercise and Evaluation Program (HSEEP)*.
- **WaterISAC.** *12 Cybersecurity Fundamentals for Water and Wastewater Utilities*. Dec 2024.
- **WaterISAC.** *Cybersecurity Fundamentals for Water and Wastewater Utilities: Small Systems Guidance Compendium*. 2025.
- **Australian Signals Directorate / Australian Cyber Security Centre.** *Protect Yourself: Multi-Factor Authentication*. Updated 21 Aug 2026.
- **Australian Signals Directorate / Australian Cyber Security Centre.** *Multi-factor Authentication: Switch it on.* 01 Sep 2026.
- **Meyer, Lucas A., et al., Microsoft Research.** *How effective is multifactor authentication at deterring cyberattacks?* May 2023.
- **UK National Cyber Security Centre.** *Disruptive cyber activity highlights risk from internet-exposed systems and edge devices*. 27 Aug 2026.
- **UK National Cyber Security Centre.** *Institutional Wilful Blindness*. *NCSC Cyber Series*, Series 3, Episode 2. 2026.
- **Cybersecurity and Infrastructure Security Agency.** *Use Logging on Business Systems*.
- **Tribal-ISAC.** *The Pulse: The State of Cybersecurity Within Tribal Nations*. 2025.
- **Baltimore City Department of Public Works.** *FY 2019 & FY 2020 Biannual Report*. See ransomware recovery and alternate operating procedures.
- **JumpCloud.** *Incident Response Statistics to Know in 2025*. 2025. Used as a secondary source for the reported cybersecurity tabletop exercise statistic; the source attributes it to CISA.
- **Omdia / Object First.** *Recovery Without Compromise: The Data-Backed Case for Backup Storage with Absolute Immutability.* Object First-sponsored research, 2026. See also Object First's 01 Sep 2026 release, which summarizes the commissioned research.

Gate 15 Resources

- **Gate 15.** *Weekly Security Sprint EP 172. Alphabet Soup Month, Cyber Protections, Leadership Engagement, and More!* Sep 2026.
- **Gate 15.** *Cyber Tabletop Exercises: Creating Your Own TTX to Engage Both the Executive and Technical Teams.* Gate 15 presentation, delivered at the TribalHub 6th Annual Cybersecurity Summit.
- **Gate 15.** *Cybersecurity: Threats & Mitigation*. Gate 15 presentation, delivered at the TribalHub Regional Tribal Technology Forums, 2026.
- **The Gate 15 Interview.** *Andy Jabbour with Adam Gruszczynski, IT Director, Potawatomi Casino Hotel*. Recorded 27 August 2026. Public podcast available as of 14 September 2026 on *Spotify*, *Apple*, and other popular podcast platforms.