Cyber Resilience Playbook

INSURICA®
HEALTHCARE

An Assurex Global Partner

Introduction

Purpose:

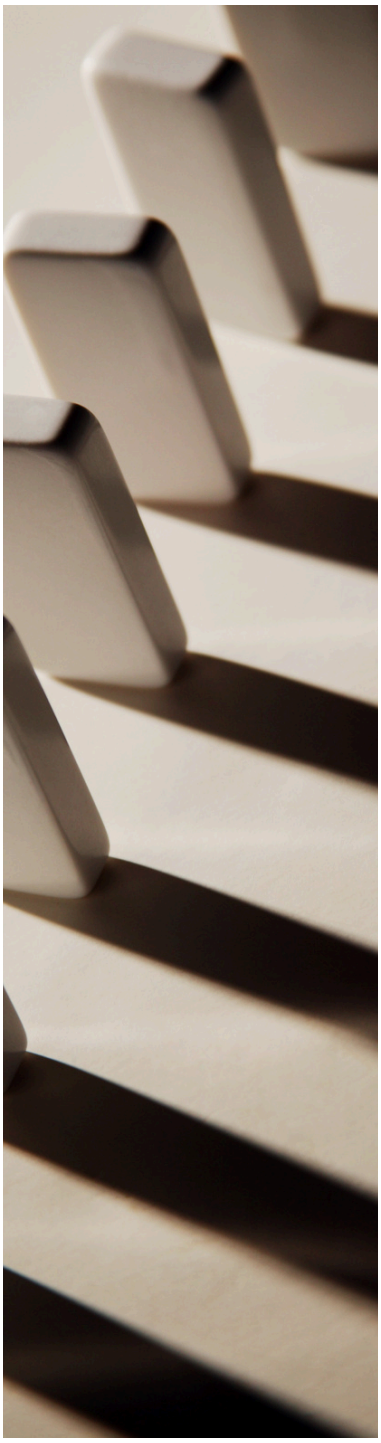
The mission of long-term care organizations extends far beyond operations, it's about creating communities where residents feel safe, cared for, and respected, and where families trust that their loved ones are protected.

This playbook is designed to help leadership align their internal teams, IT providers, vendors, and cyber insurance strategy into a coordinated, proactive framework to reduce cyber exposure, accelerate recovery, and preserve quality of care in the face of digital disruption.

What's At Stake:

When EHRs go down, billing stops, compliance flags emerge, and care delivery falters. Every hour of downtime increases risk to residents, regulatory standing, and reimbursement flow.

Section 1: Aligning Your Teams



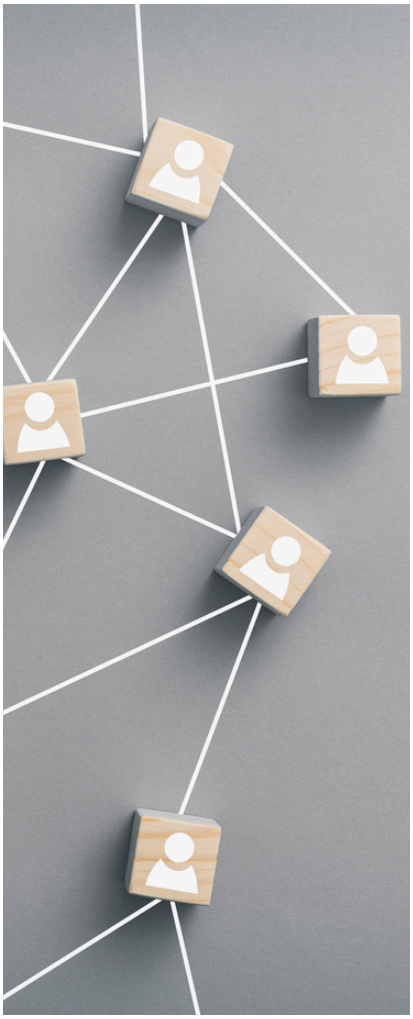
Why this matters:
In many organizations, cybersecurity, IT, leadership, and insurance function in isolation. When these groups operate independently, gaps in coverage, delays in response, and missed opportunities for cost savings or support often result. Aligning all stakeholders ensures a unified strategy, maximizes value from existing partners, and improves coordination during a cyber incident or recovery effort.

A strong cyber response doesn't begin with a breach, it begins with alignment. Cyber risk isn’t just an IT problem; it touches every aspect of your operation. Medication management, resident documentation, scheduling, payroll, compliance, communications and even building access all rely on interconnected systems. That means everyone, from CNAs to CEOs, has a role to play in resilience.

In This Section:
Discover how to bring leadership, IT, compliance, and insurance into one conversation. Learn how shared KPIs, common language, and coordinated escalation plans can break silos and turn fragmented efforts into a unified cyber strategy.

1.1 Define Roles and Communication Channels

- Create a centralized cybersecurity team (or designate a cyber lead).
- Establish regular communication between:
  - IT Department / MSP
  - Risk Management
  - Insurance Broker
  - Compliance Officer
  - Executive Leadership



Consider a recurring meeting cadence, monthly, bi-monthly, or quarterly, focused on:

- Vendor vulnerability and cloud dependency updates
- Changes to internal systems or processes
- Recent cyber threats or emerging risks
- Review of incident response preparedness
- Cross functional training opportunities

1.2 Audience Segmentation

- Develop a basic glossary of cyber terms so stakeholders speak a common language (e.g., MFA, EDR, IRP, segmentation).
- Define clear performance indicators that matter to each team:
  - IT: % of devices covered by EDR
  - Risk/Compliance: Staff training participation rate
  - Executive/Board: Time-to-recovery after outage
  - Insurance: Documented controls impacting premium/coverage
- Align metrics with both operational goals and insurance requirements to eliminate silos and track progress over time.

Suggestions:

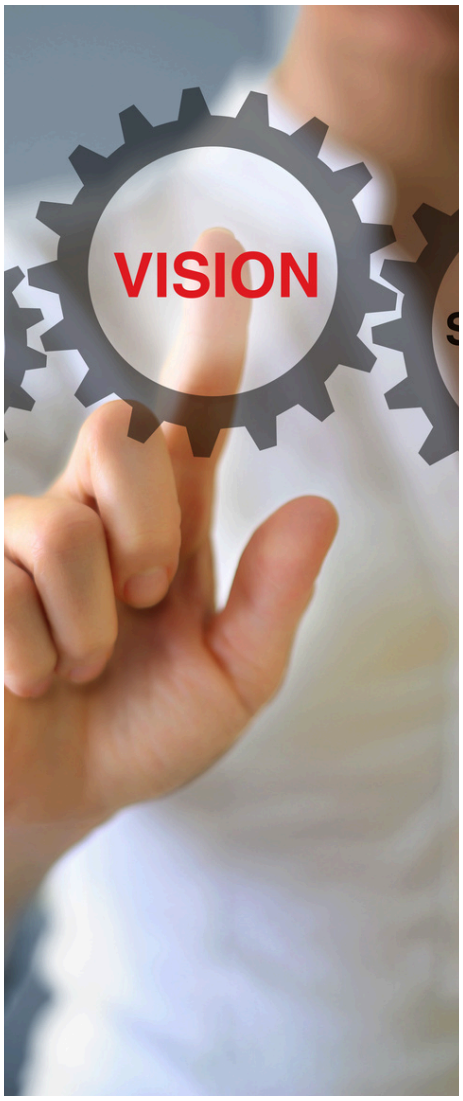
Create a simple glossary or “cheat sheet” of key cybersecurity and insurance terms; circulate it among leadership, compliance, and frontline supervisors.

Introduce shared dashboards or quarterly metric reviews to track resilience progress.

Encourage your insurance partner or IT provider to help define which metrics impact underwriting or service outcomes.

1.3 Shared Goals and Escalation Framework

- Clarify collective goals:
  - Reduce cyber risk
  - Improve response time
  - Protect patient data and resident care
- Build a basic decision matrix that outlines:
  - Who gets alerted when suspicious activity is noticed (include frontline roles like CNAs)
  - What triggers an escalation (e.g., multiple failed logins, system lag, phishing email)
  - Who is responsible for each decision during an incident (e.g., disconnecting a system, notifying leadership or law enforcement)
  - Who documents and debriefs the event
- Encourage simulation or tabletop walkthroughs of this matrix to build clarity and confidence.



Building Alignment Before the Breach

Resilience doesn't start with technology, it starts with teamwork. When leadership, IT, risk management, compliance, and insurance advisors operate in silos, vulnerabilities grow. By defining shared goals, speaking a common language, and creating clear escalation paths, organizations can eliminate confusion and strengthen coordination when it matters most.

Key Takeaways:

- Every department, from the C-suite to the front lines, plays a role in cyber preparedness.
- Regular collaboration builds awareness, improves response time, and prevents missed opportunities for support or savings.
- Measurable KPIs and shared language help teams track progress and stay aligned over time.

Next Step:

Once teams are aligned internally, the next step is optimizing your external support, especially your cyber liability insurance policy. Many LTC organizations underestimate what their policy can offer, or fail to leverage the services already built into it. Section 2 explores how to make your coverage a proactive asset, not just a safety net.

Section 2: Leveraging Cyber Liability Insurance

Why this matters:
Cyber liability insurance isn't just about transferring risk, it's a strategic lever for prevention, recovery, and financial protection. Unlike traditional insurance policies, there is no standardized ISO form for cyber. That means coverage varies significantly between carriers, and knowing what you need, and what you're actually getting, is critical.

Strong policies go beyond payouts. Many carriers now offer free services like MFA tools, breach coaching, incident response planning, and phishing simulations, yet most of these go unused.

Your broker and IT team should be aligned well before renewal. Underwriters increasingly want to meet insureds to ensure clarity and build trust. When your teams, vendors, and coverage are coordinated, insurance becomes a proactive risk management tool, not just a last line of defense.

In This Section:

- Unlock value-added services that come with your policy
- Strategically partner with your broker to align coverage with your risk profile
- Reduce premiums and enhance protection through documentation and collaboration
- Use insurance as a tool to improve system security and recovery readiness

2.1 Get More From Your Policy

- Ask about value-added services: MFA, EDR, training, breach response.
- Confirm if your carrier provides:
  - Risk assessments / vulnerability scans
  - Phishing simulations
  - Vendor management tools

Most cyber policies come with built in services that support prevention and preparedness, yet they often go unused. Leveraging them not only strengthens your internal posture but can deepen your relationship with the carrier and support your IT team at no extra cost.

Suggestions:

- Ask your broker for a list of free tools or consulting services included in your policy (some offer access to MFA, endpoint detection, breach simulations, or legal guidance).
- Assign a staff lead to ensure value-added services are explored and implemented where appropriate.
- Use these services as support for your internal team rather than a replacement, particularly helpful for under resourced IT departments.

2.2 Partnering With Your Broker

- Bring your broker into strategic planning sessions.
- Share IT policies and vendor profiles during renewals.
- Ask your broker to provide a pre-renewal coverage gap report.

Your broker isn't just a salesperson, they can serve as a strategic advisor and advocate with the carrier. Involving them early can prevent gaps, improve pricing, and build stronger alignment between your coverage and actual risks.

Suggestions:

Invite your broker to meet with your IT/security team before your renewal period.

Share updates like new vendors, cloud migrations, or plans for new communities so they can help adjust your risk profile accordingly.

Request a "pre-renewal report" to uncover any issues before the application or pricing stage.

2.3 Premium Optimization Strategy

- Document all preventive controls (MFA, EDR, backups).
- Co-complete application with IT and broker.
- Consider higher retentions or layered limits for cost control.

Underwriters reward transparency and maturity. Organizations that document their controls, demonstrate readiness and provide more than the application requires are more likely to secure favorable rates and stronger coverage terms.

Suggestions:

- Use a shared document between IT and your broker to co-author the renewal application, misreporting tech safeguards can lead to denied claims.
- Work with your broker to model different scenarios: retention increases, layered limits, or risk financing options.
- Keep a simple audit trail (screenshots, policies, completion dates) that proves your security controls are in place and active.

Turning Coverage Into Capability

Cyber liability insurance is more than financial protection, it's a bridge between risk strategy and operational execution. By tapping into the services your policy provides, aligning with your broker, and involving IT in the right conversations, you create a coverage framework that actively reduces risk. Smart organizations don't just purchase policies, they use them to their full potential.

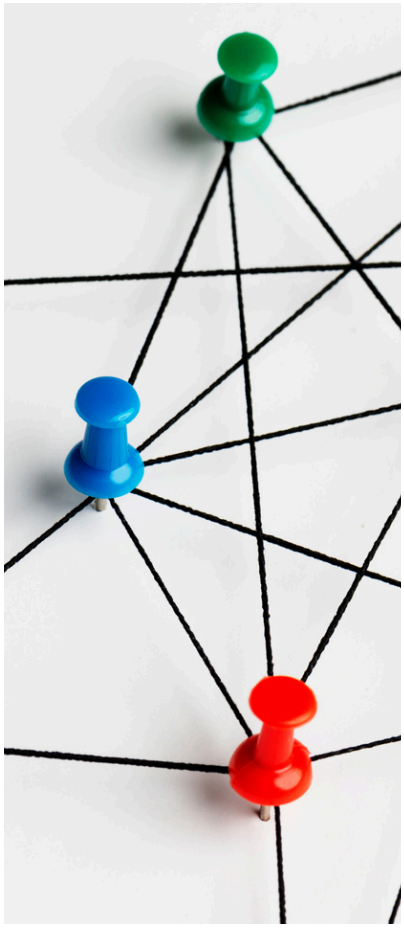
Key Takeaways:

- Many cyber policies include valuable services like often at no extra cost.
- Involving your broker and IT team early is key to better pricing and protection.
- There are no standard cyber policy forms, each carrier's coverage varies, so understanding what's included (and what's not) is critical.
- Premiums can be optimized by documenting your security posture, collaborating on applications, and considering coverage structure adjustments.

Next up: Engaging Your IT Team

Strong policies are only as effective as the systems and people behind them. In the next section, we'll explore how to make your IT team a driving force in resilience, from application accuracy to incident response leadership.

Section 3: Engaging Your IT Team



Why this matters:
Your IT team, whether in house or outsourced, is on the front lines of both prevention and response. Yet in many organizations, IT operates in the background, disconnected from strategic planning, insurance discussions, and organizational training. This disconnect can result in unmitigated vulnerabilities, slow breach response, or incomplete applications that lead to denied coverage.

Proactive, structured engagement with your IT provider ensures they're not just maintaining systems, but actively supporting your resilience strategy. Whether it's mapping digital dependencies, rehearsing response plans, or completing cyber insurance applications, their involvement is essential to preparedness and protection.

In This Section:

- How to engage IT beyond daily troubleshooting
- Why involving IT in cyber insurance can improve outcomes
- Building IRPs that include the full organization
- Running simulations that surface hidden gaps

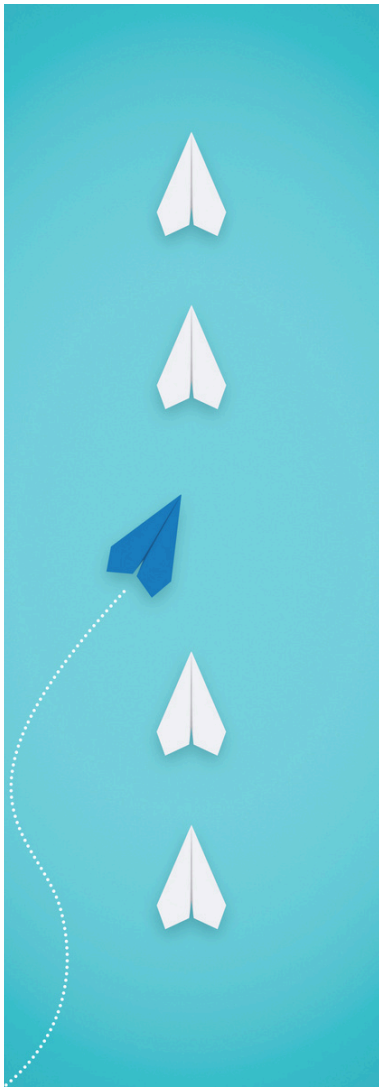
3.1 Cyber Application Support

Too many organizations treat the cyber insurance application like a form to "get through" yet every detail matters. Most questions require accurate technical validation from IT, and getting them wrong can jeopardize claims or inflate premiums.

But this isn't just about filling out a form. Every cyber upgrade, whether it's MFA deployment, new firewall software, or backup changes, should trigger a conversation with both your IT team and your cyber aligned leadership group. Coordinating these changes ensures everyone understands their role and that upgrades translate into improved coverage and risk posture.

Suggestions:

- Always co-complete cyber insurance applications with IT.
- Loop in your cyber alignment team (from Section 1) to vet and validate changes that impact your security posture.
- Create a simple "update notification" checklist for IT to notify the cyber team of upgrades or tool integrations that might affect documentation, training, or incident response.



3.2 Incident Response Protocols

Many LTC organizations don't have scenario based incident response plans. Having one IRP that covers everything from a system outage to a ransomware attack is not enough.

Effective IRPs should be tailored to the most likely disruptions you might face:

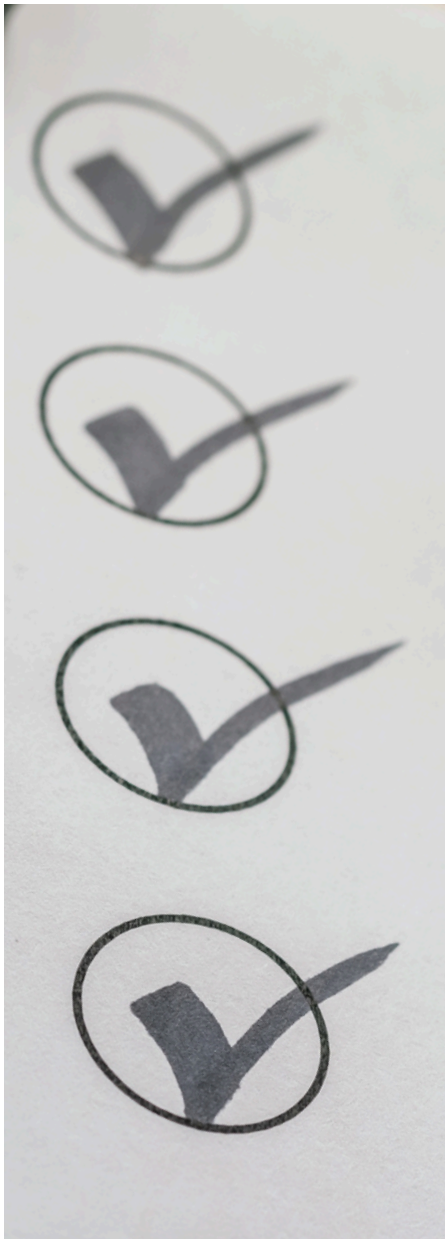
- Internet provider failure
- Suspected internal breach (e.g., unauthorized access)
- Third-party/vendor outage or breach
- Natural disaster triggered network issues

These plans should clearly outline the first five minutes after an alert, who notices, who reports, who decides, and what's done. Everyone from CNAs to the administrator may have a role.

Suggestions:

- Develop or expand IRPs for each distinct scenario.
- Include visual "first response maps" to guide staff decisions.
- Train CNAs and frontline roles on basic red flags (e.g., slow EHR access, device behaving abnormally, system message anomalies).
- Coordinate IRP development with your cyber team and broker to align with coverage conditions and legal notification standards.

3.3 Testing and Simulation



Go beyond IT, include everyone

Simulations are one of the most powerful but underused tools in LTC. They surface confusion, gaps, and slowdowns before something goes wrong. Most organizations run IT only simulations (if any at all). But in healthcare, it's the nurses, caregivers, schedulers, and receptionists who will be the first to notice if a system fails.

Effective simulations should:

- Include all departments, not just IT.
- Test not just recovery but also early detection and escalation.
- Be used to refine incident response plans and boost team confidence.

Suggestions:

- Start with short, 15–20 minute tabletop exercises for different teams.
- Rotate scenarios (internet outage, EHR breach, vendor failure, etc.).
- Debrief each simulation and update the IRP accordingly.
- Include scenarios for breach detection: What does a phishing email look like? What if you see files disappearing or a lockout message?

Turn IT Into a Resilience Ally

Your IT team can do far more than troubleshoot, they can be architects of resilience. When engaged fully, they help validate insurance applications, support incident response, and test readiness across the organization. Just as important, they can guide frontline training and ensure upgrades are leveraged for both protection and premium advantage.

Key Takeaways:

- Cyber applications require accurate technical input, don't go it alone.
- Build IRPs around scenarios, not just general concepts.
- Simulations reveal hidden weaknesses, but only if everyone's involved.

Next Up: Coordinating With Vendors

No matter how strong your internal strategy is, third-party gaps can become your weakest link. In the next section, we'll explore how to evaluate your vendors, clarify responsibilities, and build redundancy into your most critical systems.

Section 4: Coordinating With Vendors

Why this matters:
Your cybersecurity strategy is only as strong as your weakest third-party. Many LTC organizations rely on cloud hosted software, outsourced IT, and specialized vendors for critical operations, but fail to assess the risks that come with those dependencies.

Coordinating with vendors isn't just about maintaining uptime. It's about understanding their security, knowing what liabilities you're assuming in contracts, and having realistic recovery plans in case something goes wrong.

Too often, vendor due diligence is skipped, contract language is boilerplate, and accountability is vague. In an incident, this creates confusion, blame shifting, and unnecessary delays. By proactively evaluating vendor resilience and negotiating fair, protective agreements, leaders can reduce risk, ensure continuity, and improve leverage in breach or service failure scenarios.

In This Section:

- How to assess and prioritize vendor risk
- What to look for in IT and EHR contracts
- Questions to ask to ensure accountability and redundancy

4.1 Cloud Dependency Map

Not all systems are created equal, and not all have offline functionality. Knowing which platforms are cloud-dependent helps you prioritize recovery and redundancy.

This map is the foundation for emergency planning. Use it to develop contingency plans, paper backups, and staff training tailored to each system. This will empower staff to respond efficiently during an outage, minimizing disruptions to care and operations. Additionally, encourage feedback to refine your strategies, while building resilience and responsiveness.

Suggestions:

- Categorize each system: clinical, operational, financial, resident facing
- Rank by business-criticality (e.g., EMAR > payroll > timeclock)
- Ask vendors:
  - What happens if your platform is inaccessible for 12+ hours?
  - Do we have downloadable backups, PDFs, or local access modes?

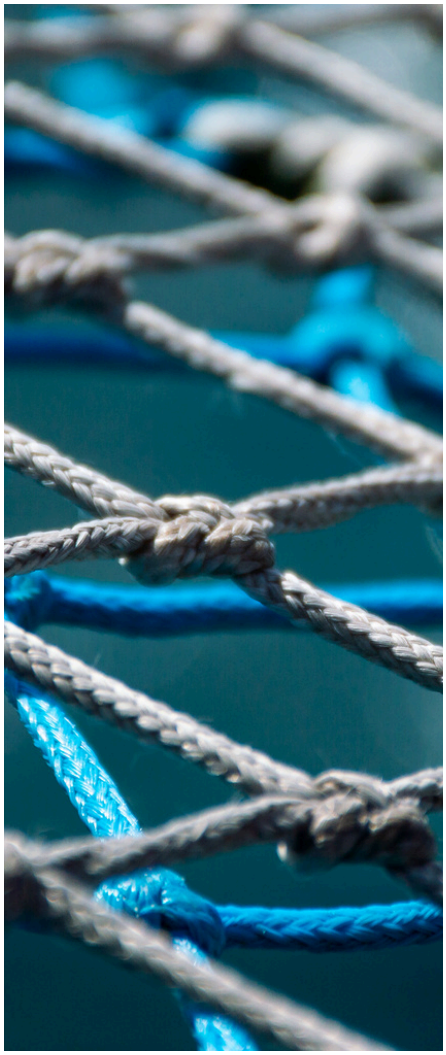
4.2 Third-Party Risk Review

Your vendors' weaknesses can quickly become your crisis. Contracts with IT providers, EHR platforms, billing services, and other vendors should be reviewed not just for cost and functionality, but for cyber resilience. Look for service level agreements (SLAs) that specify breach notification timelines, system recovery commitments, and shared liability. Unfavorable clauses can leave you exposed or delay your recovery. Having legal, IT, and leadership jointly review these agreements ensures you're not unknowingly accepting unreasonable risk or signing away your leverage in a crisis.

Suggestions:

- Review SLAs: What's guaranteed for breach response or downtime?
- Require vendors to maintain their own cyber liability coverage
- Look for:
  - Indemnification clauses protecting you from vendor caused harm
  - Notification requirements for system changes or breaches
  - Right-to-audit language (especially for tech vendors or MSPs)

4.3 Redundancy Planning



Redundancy isn't a luxury, it's a resilience requirement. Even short term disruptions can put resident safety, medication accuracy, and documentation at risk. Planning ahead means identifying not only what systems are mission-critical but how to maintain continuity if those systems go down. Resilient organizations build backup pathways before they're needed, whether it's an offline MAR, a local server that mirrors key cloud data, or a standing agreement with a secondary tech partner who can step in if the primary MSP is overwhelmed or compromised.

This isn't about adding unnecessary vendors or infrastructure, it's about identifying the most cost effective fail safes that protect operations and resident care when the unexpected happens.

Suggestions:

- Identify systems with no paper alternative, develop one
- Designate primary and backup IT vendors/MSPs
- Pre-plan how data will be recovered, restored, or transitioned

Build a Safety Net Beyond Your Walls

The strength of your cybersecurity posture is deeply tied to your vendor ecosystem. From cloud hosted EHR platforms to outsourced MSPs, every external partner introduces both value and risk. That's why due diligence, contractual clarity, and redundancy planning are essential, not just for IT continuity, but for resident safety and regulatory compliance.

Key Takeaways:

- Cloud reliance must be mapped and prioritized based on impact and recovery needs.
- Vendor contracts should be reviewed for fairness, liability allocation, and realistic response expectations.
- Backup systems and alternate support vendors are vital to maintain operations during outages or vendor failures.
- Proactive vendor assessments help surface hidden risks and ensure your expectations are aligned with their capabilities.

Next Up: Your Roadmap to Resilience

In our final section, we'll tie it all together with a quarterly action plan that makes implementation manageable and measurable, helping your organization move from reactive to resilient.

Section 5: Your Roadmap to Resilience

Why this matters:
Cyber resilience isn't a one size fits all journey. Some organizations are just beginning to centralize their cyber efforts; others have IT protocols but lack vendor alignment or insurance integration. Different starting points require different strategies.

This section offers a phased approach to help you move from vulnerability to preparedness, without overwhelming your team. Whether you're building foundational capabilities or refining mature processes, a structured roadmap ensures accountability, progress, and protection.

In This Section:

- Three roadmap templates based on organizational readiness and capacity
- Key actions tailored to each roadmap
- Tips for adapting milestones to your team size and resources

How To Use This Section:
This isn't a checklist to complete, it's a framework to adapt.
Every organization starts from a different place. Some are building from the ground up. Others are refining and coordinating existing efforts. The tracks that follow are designed to guide, not dictate, your path forward.

Tips For Getting Started:

- Choose a track that most closely aligns with your current capabilities, not where you want to be, but where you are today.
- Adjust as needed. These roadmaps are flexible. Use them to shape your timeline, assign responsibilities, and pace your progress.
- Focus on priorities. Don't try to do everything at once. Each quarter is about progress, not perfection.
- Leverage your team. Revisit Section 1 and ensure your internal stakeholders are aligned and engaged.

Remember: The goal isn't to "check every box." The goal is to create a living, evolving plan that reduces risk, improves coordination, and builds resilience over time.

Track A: Foundational Readiness

For organizations just beginning to formalize their cyber resilience strategy

Quarter	Key Milestones
Q1	- Identify core team (IT, risk, leadership, broker) - Schedule recurring cyber coordination meetings - Inventory cyber insurance coverage and value added services
Q2	- Co-complete cyber application with IT & broker - Create basic IRP playbook (internet down, suspected breach) - Map mission critical vendors and cloud reliance
Q3	- Hold first tabletop simulation - Begin internal cyber policy reviews - Review vendor contracts for SLAs & breach response clauses
Q4	- Conduct a basic internal risk assessment - Build Year 2 roadmap with input from IT, vendors, and broker

Track B: Operational Integration

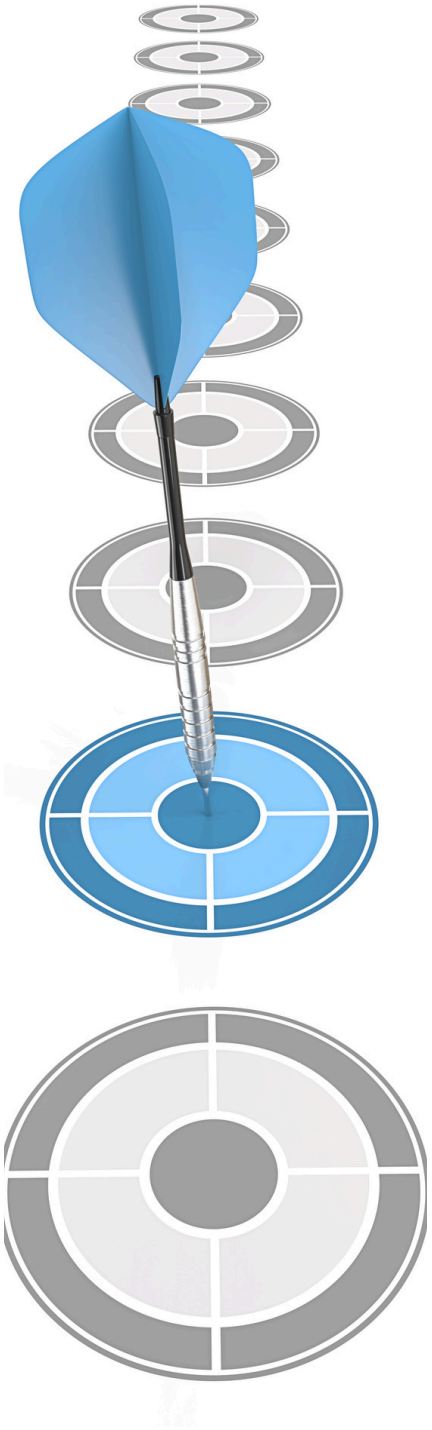
For organizations with some controls in place but limited cross team coordination

Quarter	Key Milestones
Q1	- Expand cross functional cyber team and set shared KPIs - Conduct insurance gap analysis and document preventive controls - Validate IRP covers multiple threat scenarios
Q2	- Update cyber insurance strategy: retention levels, layered limits - Coordinate IT/vendor meeting to review access points & system dependencies - Begin phishing training or cyber hygiene modules
Q3	- Perform full contract audit on top 5 vendors - Test downtime protocols with operations & nursing - Align cyber KPIs to board reporting dashboard
Q4	- Launch formalized response escalation matrix - Co-review cyber coverage and claims process with carrier - Plan next year's simulations and staff training cadence

Track C: Strategic Resilience Leadership

For organizations ready to lead in cyber preparedness and influence industry standards

Quarter	Key Milestones
Q1	- Launch “Cyber Resilience Council” with defined charter - Conduct gap analysis against HICP or NIST standards - Build escalation protocol that includes CNA level observations
Q2	- Complete system wide downtime simulation - Formalize backup MSP/vendor agreements - Develop “Red Flag” recognition training for all staff levels
Q3	- Co-host cyber resilience workshop with broker or IT vendor - Implement automated cyber KPI dashboard - Engage legal counsel to optimize vendor indemnification language
Q4	- Publish internal cyber audit report with board brief - Test multi-scenario IRPs (ransomware, vendor breach, internal compromise) - Develop 3 Year strategic cyber roadmap



Turning Planning Into Practice

Every organization has different challenges, timelines, and capacities, but every organization benefits from progress. Whether you're taking first steps or refining a sophisticated program, what matters most is that cyber resilience becomes part of your operational culture, not a separate initiative.

Key Takeaways:

- You don’t need to do everything at once, start where you are, but don’t stay there.
- Cyber resilience is a shared responsibility; align leadership, IT, vendors, and frontline staff.
- Roadmaps bring structure, but your adaptability will determine success.
- A stronger cyber posture improves regulatory readiness, staff confidence, and resident safety.

Next Steps:

- Choose the roadmap that most closely reflects your current state.
- Set quarterly goals, assign owners, and build accountability across departments.
- Bring this playbook into your leadership meetings, and invite others to co-own the journey.

Need Help Navigating Your Cyber Resilience Journey?

Whether you're just getting started, facing a specific challenge, or looking to take your efforts to the next level, I'm here to help.

As part of INSURICA’s healthcare practice, I work with long-term care leaders to develop strategies that go beyond insurance, aligning operations, technology, and risk management into a proactive framework that increases control and drives more predictable outcomes.

If you’d like support walking through this playbook with your team, want to explore customized assessments or tabletop exercises, or simply need a second set of eyes on your current approach, I’d be happy to connect.

Drew.Colwell@INSURICA.com
406-991-1727

INSURICA HEALTHCARE

An Assurex Global Partner