YAKAMICHI INTELLIGENCE CENTRE

PLAYBOOK 02 • RESTORED PUBLICATION

Cyber Resilience

An executive operating playbook for anticipating, withstanding, recovering from and adapting to severe cyber disruption.

UNDERSTAND	PROTECT	CONTAIN	CONTINUE	RECOVER	ADAPT
Critical services	Reduce exposure	Limit blast radius	Sustain operations	Restore safely	Improve

EXECUTIVE PURPOSE

Move cybersecurity beyond control compliance toward demonstrable operational resilience. This playbook integrates cyber defense, business continuity, recovery, crisis leadership and supplier assurance.

YAKAMICHI PERSPECTIVE

The objective is not to promise that disruption will never occur. It is to ensure disruption does not become organizational paralysis.

Contents & How to Use This Playbook

How to Use It

- Boards and executives: establish resilience priorities, tolerances, crisis authority and investment decisions.
- CISOs and technology leaders: connect security architecture to critical-service recovery and containment.
- Business continuity and operations leaders: align workarounds and recovery priorities with cyber scenarios.
- Legal, communications, risk and suppliers: use shared scenarios and decision records so response is coordinated.

DESIGN PRINCIPLE

Assume prevention can fail. Resilience is the combination of reducing likelihood, limiting consequence, sustaining essential operations and recovering safely.

CHAPTER 01

Executive Resilience Mandate

Cyber resilience is an enterprise capability. A serious cyber event can simultaneously become a technology outage, operational interruption, legal matter, customer crisis, financial event and leadership test.

The Six-Part Yakamichi Framework

Understand Identify critical services, dependencies, threat scenarios and acceptable disruption.

Protect Apply proportionate controls to identities, endpoints, networks, cloud, data and suppliers.

Contain Segment environments and establish rapid isolation so compromise does not spread.

Continue Maintain minimum viable operations, workarounds and alternate communications.

Recover Protect recovery assets and restore according to business-service priority.

Adapt Use incidents, exercises and intelligence to improve architecture and readiness.

Leadership Responsibilities

- Define which services cannot tolerate prolonged interruption.
- Approve disruption tolerances and major resilience investments.
- Ensure cyber crisis authority is explicit before an incident.
- Require evidence that recovery works under realistic conditions.
- Track unresolved resilience gaps and concentration risks.

EXECUTIVE TEST
Can the enterprise still make decisions and deliver its most important services if identity, email, primary cloud services or a critical supplier is unavailable?

CHAPTER 02

Critical Services & Impact Tolerances

Asset inventories are necessary, but resilience begins with business outcomes. Leaders should identify the services whose interruption would create material customer, safety, regulatory, financial or strategic harm.

QUESTION	OUTPUT
What must continue?	Prioritized critical-service catalogue
How long can it be unavailable?	Maximum tolerable disruption
What minimum service is acceptable?	Minimum viable operating level
What supports it?	People, data, technology, facility and supplier map
Who owns the outcome?	Named executive/business service owner

Dependency Mapping

- Applications, infrastructure, networks and cloud regions.
- Identity providers, privileged accounts and administrative tooling.
- Critical data stores, keys, certificates and recovery credentials.
- Specialist personnel, facilities and telecommunications.
- Third parties, SaaS platforms, managed service providers and upstream suppliers.

CONCENTRATION RISK

Different services can appear independent while sharing the same identity platform, cloud provider, network, administrator or supplier. Map common dependencies, not only direct ones.

CHAPTER 03

Threat Scenarios & Exposure

Resilience planning should be scenario-led. The question is not whether a specific attack prediction is correct, but whether the organization has prepared for plausible conditions that remove critical capabilities.

SCENARIO	RESILIENCE QUESTION
Ransomware / destructive malware	Can priority services operate while large portions of the environment are isolated?
Identity compromise	Can administrators recover if primary identity is untrusted?
Cloud / SaaS outage	Are alternate processes available for critical services?
Data integrity attack	Can trusted data be identified and restored?
Supplier compromise	Can the enterprise isolate or replace the dependency?
Communications outage	Can leadership coordinate without normal email/chat/voice?

Exposure Assessment

- Likelihood and threat relevance.
- Business consequence and velocity.
- Existing preventive and detective controls.
- Containment options and time to isolate.
- Continuity workaround and recovery evidence.
- Residual risk and executive decision required.

SCENARIO DISCIPLINE

Use a small number of severe but plausible scenarios to test the whole enterprise. Avoid exercises where every backup, person and communication channel conveniently remains available.

CHAPTER 04

Identity, Access & Privileged Resilience

Identity is often the control plane for modern infrastructure. If identity is compromised, attackers may gain access to cloud, endpoints, backups, collaboration platforms and recovery systems at once.

CONTROL	RESILIENCE EXPECTATION
Strong authentication	Phishing-resistant methods for privileged and high-risk access where appropriate
Privilege	Separate administrative identities; minimize standing privilege
Break-glass access	Protected emergency identities with monitored, tested procedures
Recovery	Offline/protected recovery credentials and documented identity restoration
Service accounts	Inventory, least privilege, secret rotation and ownership
Administration	Dedicated hardened administrative pathways for critical systems

Executive Questions

- Can we administer recovery systems if normal identity services are unavailable?
- Are backup administrators separated from ordinary domain/cloud administrators?
- Who can invoke emergency access and how is it monitored?
- Have identity recovery procedures been tested, not merely documented?

IDENTITY PRINCIPLE
A resilient backup is of limited value if the credentials required to restore it are compromised or inaccessible.

CHAPTER 05

Containment, Segmentation & Blast-Radius Control

Resilience depends on preventing a local compromise from becoming an enterprise-wide failure. Containment must be designed into architecture and practiced operationally.

AREA	CONTROL OBJECTIVE
Network	Separate critical environments and restrict unnecessary east-west movement
Identity	Limit privilege propagation and administrative trust relationships
Endpoints	Rapidly isolate compromised devices without losing enterprise visibility
Cloud	Separate accounts/subscriptions/projects and control cross-environment trust
Backups	Keep recovery environments isolated from production compromise
Suppliers	Restrict third-party access by system, time and privilege

Rapid Isolation Decisions

- Which systems can security isolate without executive approval?
- Which services require business-owner coordination before shutdown?
- What conditions justify disconnecting a site, supplier or cloud integration?
- How will evidence be preserved while urgent containment occurs?
- How will critical operations continue after isolation?

BLAST-RADIUS TEST

Architecture should assume one control fails. Ask what an attacker can reach next, what privilege they inherit and how quickly defenders can sever that path.

CHAPTER 06

Backup, Recovery & Technology Restoration

Backups are not the same as recoverability. Restoration requires trusted data, working credentials, clean infrastructure, correct sequencing, adequate capacity and business validation.

RECOVERY LAYER	EVIDENCE REQUIRED
Backup integrity	Protected/immutable copies and monitoring of backup failures
Isolation	Recovery assets separated from production compromise
Restoration	Routine test restores under realistic conditions
Sequencing	Identity, network, data and applications restored in dependency order
Clean environment	Ability to rebuild into trusted infrastructure
Business validation	Service owner confirms restored service is usable and data is trustworthy

Recovery Priorities

- Restore the control plane needed to administer recovery safely.
- Prioritize critical business services rather than server-by-server convenience.
- Validate data integrity before returning consequential services.
- Preserve forensic evidence while avoiding unnecessary delay to safe restoration.
- Record actual recovery times and compare them with business tolerances.

RECOVERY PRINCIPLE
The best recovery plan is one that has survived contact with a realistic test.

CHAPTER 07

Cyber Crisis Leadership & Communications

During severe incidents, uncertainty rises while decision time shrinks. Executives need a practiced structure for authority, escalation, legal judgment, stakeholder communication and operational trade-offs.

ROLE	CRISIS ACCOUNTABILITY
Executive Incident Lead	Enterprise priorities and major trade-offs
Cyber / Technology	Technical containment, evidence and recovery
Operations	Critical-service continuity and business impact
Legal / Privacy	Privilege, regulatory and notification analysis
Communications	Employees, customers, media and stakeholder messaging
Risk / Insurance	Exposure, insurer coordination and decision records

Decisions to Pre-Authorize

- Isolation or shutdown of critical technology.
- Activation of alternate communications and crisis facilities.
- Engagement of external incident-response, legal and forensic support.
- Regulatory/customer notification governance.
- Business workaround activation and service prioritization.
- Conditions for restoration and return to normal operations.

COMMUNICATIONS RESILIENCE

Assume normal email and collaboration systems may be unavailable or untrusted. Maintain tested alternate executive communication channels and current contact information.

CHAPTER 08

Third-Party Security, Supply Chain Risk & Cloud Assurance

The enterprise can outsource technology but not operational consequence. Critical suppliers should be governed according to the services they support, the access they hold and the time available to replace them.

AREA	ASSURANCE EXPECTATION
Criticality	Classify suppliers by business consequence, not only spend
Access	Control and monitor privileged/vendor access
Security	Obtain evidence proportionate to criticality and exposure
Incident notice	Define prompt notification and coordination obligations
Resilience	Understand recovery capability, dependencies and concentration
Cloud	Map identity, region, data, backup and shared-responsibility dependencies
Exit	Maintain data retrieval, transition and substitution options

Supply-Chain Questions

- Which critical suppliers share the same cloud, software or telecommunications dependency?
- Can a provider remotely administer systems during an incident?
- What happens if the provider is operational but our connection to it is not?
- Can we continue if a critical SaaS platform is unavailable for several days?
- Have supplier failure scenarios been exercised with business owners?

FOURTH-PARTY RISK

Seek visibility where downstream dependencies can create material enterprise consequences. The goal is not an infinite supplier map, but awareness of consequential concentration.

CHAPTER 09

Exercises, Metrics & Continuous Assurance

Resilience becomes credible through evidence. Exercises should test decisions and dependencies; metrics should reveal operational capability rather than security activity alone.

METRIC	EXECUTIVE MEANING
Critical services with tested recovery	Coverage of demonstrated resilience
Recovery time achieved vs tolerance	Whether capability matches business need
Backup restoration success	Whether recovery assets actually work
Critical dependency coverage	Visibility of hidden single points of failure
High-risk supplier exposure	External concentration and assurance
Overdue exercise findings	Whether lessons become improvements
Time to executive decision	Crisis leadership readiness

Exercise Ladder

Tabletop Walk through roles, assumptions and decisions.

Functional Use real teams, communications and procedures.

Technical recovery Restore systems/data in realistic sequence.

Integrated enterprise exercise Combine cyber, operations, legal, communications and suppliers.

ASSURANCE RULE
Findings are not closed because a document was updated. Close them when the underlying capability has been implemented and, where material, retested.

CHAPTER 10

180-Day Cyber Resilience Program

WINDOW	PRIORITY	DELIVERABLES
0–30 Days	Establish baseline	Critical services; executive sponsor; major scenarios; recovery evidence review
31–60 Days	Map dependencies	Applications, identity, infrastructure, data, people, facilities and suppliers
61–90 Days	Validate recovery	Restore priority services; verify protected backups; test privileged recovery access
91–120 Days	Exercise enterprise	Cross-functional cyber crisis exercise with executive participation
121–150 Days	Close critical gaps	Containment, communications, supplier and recovery remediation
151–180 Days	Institutionalize	Board reporting, recurring exercises, metrics and funded improvement roadmap

Success at Day 180

- Critical services and tolerances are approved.
- Major technology and supplier dependencies are mapped.
- Identity and backup recovery have been tested.
- Containment authorities and procedures are explicit.
- Alternate executive communications are operational.
- A cross-functional cyber crisis exercise has been completed.
- Material findings have owners, dates and executive visibility.

PROGRAM PRINCIPLE

Prioritize evidence over paperwork. The first six months should prove the enterprise can contain, continue and recover, not merely produce a larger resilience library.

APPENDIX A

Critical Service Resilience Record

FIELD	RECORD
Service	Name and business owner
Purpose	Customer / regulatory / operational outcome
Maximum tolerable disruption	____ hours / days
Minimum viable level	Essential functions during disruption
Technology dependencies	Applications, identity, network, cloud, data
People / facility dependencies	Critical roles and locations
Third parties	Critical providers and concentration
Workaround	Manual / alternate process
Recovery evidence	Last test, achieved time, issues
Residual gaps	Owner and remediation date

APPENDIX B

Cyber Crisis Decision Log

TIME	DECISION	RATIONALE / EVIDENCE	OWNER	REVIEW
____	Isolate / continue / restore / notify	_____	_____	____
____	_____	_____	_____	____
____	_____	_____	_____	____
____	_____	_____	_____	____

Record material decisions, information available at the time, dissent/uncertainty where relevant, accountable authority and any required review point.

APPENDIX C

Recovery Validation Checklist

- ☐ Protected/immutable recovery copies available
- ☐ Recovery credentials accessible through protected path
- ☐ Clean restoration environment available
- ☐ Identity/control-plane restoration sequence validated
- ☐ Critical data integrity checked
- ☐ Application dependencies restored in correct order
- ☐ Business owner validates minimum viable service
- ☐ Actual restoration time recorded
- ☐ Forensic/evidence requirements considered
- ☐ Lessons and remediation assigned

RESTORATION GATE
Do not equate technical startup with business recovery. The service owner should validate that the restored capability is trustworthy and usable.

APPENDIX D

Executive Cyber Exercise Template

ELEMENT	DESIGN
Scenario	Severe but plausible disruption tied to critical services
Opening condition	What is known, unknown and unavailable
Escalation injects	Identity loss, supplier failure, data leak, media/regulatory pressure
Decisions	Isolation, continuity, notification, recovery priority
Participants	Executives, cyber, technology, operations, legal, communications, suppliers
Evidence	Decision times, gaps, assumptions and control failures
After action	Prioritized findings, owners, due dates and retest criteria

Exercise Questions

- What would leadership decide with incomplete information?
- Which normal communication or identity assumptions fail?
- What critical service becomes unavailable first?
- Which supplier or recovery dependency surprises the team?
- What decision cannot wait for perfect technical certainty?

APPENDIX E

Board & Executive Resilience Dashboard

INDICATOR	CURRENT	TREND	ACTION THRESHOLD
Critical services with tested recovery	___%	↑ / → / ↓	Target ___%
Recovery within approved tolerance	___%	↑ / → / ↓	Escalate below ___%
Successful backup restore tests	___%	↑ / → / ↓	Target ___%
Critical supplier resilience coverage	___%	↑ / → / ↓	Target ___%
Overdue material findings	___	↑ / → / ↓	Escalate above ___
High-risk concentration exposures	___	↑ / → / ↓	Decision required
Executive exercise decision time	___ min	↑ / → / ↓	Target ___
Residual risks outside appetite	___	↑ / → / ↓	Decision required

YAKAMICHI INTELLIGENCE CENTRE

APPENDIX F

Cyber Resilience Maturity Model

LEVEL	CHARACTERISTICS	EXECUTIVE MEANING
1 — Reactive	Siloed security/recovery; plans largely untested	High uncertainty during disruption
2 — Developing	Critical assets identified; basic exercises and recovery tests	Capability exists but is uneven
3 — Managed	Service mapping, tested recovery and executive exercises	Predictable response to major incidents
4 — Adaptive	Continuous assurance, scenario testing, telemetry and learning	Resilience supports strategic confidence

Executive Checklist

- ☐ Critical business services and tolerances defined
- ☐ Technology and third-party dependencies mapped
- ☐ Cyber crisis authority and escalation paths documented
- ☐ Immutable/protected backups and restoration tested
- ☐ Alternate communications available
- ☐ Priority recovery sequence validated
- ☐ Executive cyber exercise completed within last 12 months
- ☐ Material findings tracked to closure
- ☐ Board receives resilience metrics, not only security metrics
- ☐ Lessons from incidents and exercises feed investment decisions

Yakamichi Perspective

Organizations that connect cybersecurity with continuity, recovery, supplier assurance and executive crisis leadership are better positioned to protect intelligence, sustain operations and make confident decisions under pressure.

REQUEST A CONFIDENTIAL CONSULTATION

United States: +1 202 413 3763 | Maryland, USA
Nigeria: +234 811 095 0651 | Abuja, Nigeria

YAKAMICHI • Artificial Intelligence • Cybersecurity • Counter-Surveillance • Corporate Risk Intelligence