YAKAMICHI INTELLIGENCE CENTRE

EXECUTIVE BRIEFING 08

Executive Incident Response Playbook

Leading decisively when a cyber incident becomes a business crisis.

DETECT	CONTAIN	DECIDE	RECOVER	LEARN
Establish facts	Limit damage	Set priorities	Restore safely	Strengthen resilience

EXECUTIVE PREMISE

During a major cyber incident, the executive team's job is not to perform technical forensics. Its job is to establish authority, protect critical operations, make risk decisions with incomplete information and keep the organization aligned while specialists contain and recover the environment.

Protecting Intelligence. Securing Operations. Managing Risk.

Executive Summary

Cyber incidents become enterprise crises when they disrupt critical services, compromise sensitive information, create safety concerns, trigger legal or regulatory duties, threaten liquidity or damage stakeholder confidence. At that point, technical response alone is insufficient.

Effective incident leadership requires a predefined command structure, reliable information flows and clear decision rights. Executives must know who is in charge, which services matter most, when to escalate, how to preserve evidence, who can authorize disruptive containment actions and how communications will be coordinated.

The best time to settle these questions is before an incident. A practiced executive playbook reduces confusion and enables specialists, business leaders and advisers to work from the same priorities.

When Executive Command Is Required

- Material disruption to a critical business service or customer-facing operation.
- Confirmed or suspected compromise of sensitive, regulated or strategically important information.
- Ransomware, destructive malware, widespread identity compromise or privileged-account abuse.
- A cyber event involving a critical supplier, cloud provider or interconnected partner.
- Potential regulatory notification, litigation, public disclosure or significant reputational impact.

Executive Takeaways

1. Establish command	One accountable incident leader and one executive decision structure.
2. Separate facts from assumptions	Use confidence levels and time-stamped situation reporting.
3. Protect critical services	Business impact should drive technical priorities.
4. Coordinate communications	Legal, regulatory, employee, customer and media messages must align.
5. Preserve optionality	Avoid irreversible decisions until consequences are understood where time permits.

The Yakamichi Executive Incident Model

1. Mobilize Confirm severity, activate the incident structure, establish secure communications and bring the required technical, legal, operational and executive leaders together.

2. Stabilize Determine what is known, what is affected and which critical services or safety obligations are at risk. Authorize urgent containment where necessary.

3. Decide Frame material decisions with options, consequences, legal considerations, operational impact and decision deadlines.

4. Communicate Maintain a controlled source of truth and coordinate internal, customer, regulator, partner and public communications.

5. Recover Restore priority services using validated recovery paths. Do not trade recovery speed for reinfection or loss of evidence.

6. Learn Conduct an after-action review, assign remediation ownership and report material lessons to executive leadership and the board.

Executive Command Structure

Role	Primary Responsibility	Key Output
Executive Incident Lead	Enterprise priorities and major decisions	Decision authority
Technical Incident Lead	Containment, investigation and recovery	Technical situation
Business Operations	Service impact and continuity	Operational priorities
Legal / Privacy	Privilege, obligations and notification	Legal guidance
Communications	Stakeholder and public messaging	Approved narrative

The Executive Situation Report

Every briefing should answer six questions: What happened? What do we know with confidence? What is affected? What is the current business impact? What decisions are required now? What will happen before the next update? A short, disciplined situation report is more useful than a flood of raw technical detail.

Critical Executive Decisions

Major incidents force decisions under uncertainty. The playbook should define who can make each decision and which advisers must be consulted.

Isolate or shut down systems	Balance containment benefit against operational, safety and evidence impacts.
Invoke business continuity	Determine which alternate processes and recovery sites should activate.
Engage external specialists	Forensics, counsel, crisis communications, insurers and specialist responders.
Notify stakeholders	Assess contractual, regulatory and legal thresholds and required timing.
Public communication	Decide when silence creates more risk than controlled disclosure.
Extortion demands	Escalate to legal, sanctions, law-enforcement, insurance and executive review; never treat payment as a purely technical decision.
Return to service	Require evidence that recovery is sufficiently secure and operationally stable.

First 60 Minutes

- Confirm incident severity and executive escalation threshold.
- Activate the incident command structure and secure communications channel.
- Preserve logs, evidence and relevant system state where feasible.
- Identify critical services affected or at immediate risk.
- Restrict uncontrolled internal discussion and external statements.
- Set the next executive briefing time and assign a situation-report owner.

Common Leadership Failure Patterns

Typical failures include multiple executives issuing competing instructions, demanding certainty before acting, focusing on attribution instead of containment, communicating before facts are validated, allowing business teams to reconnect systems prematurely, and treating the event as solely an IT problem.

Executive Action Plan: Prepare Before the Incident

0–30 DAYS | Define authority

Approve severity thresholds, executive roles, escalation paths, decision rights and secure out-of-band communications.

31–60 DAYS | Build the playbook

Document critical services, contacts, external advisers, notification pathways, decision templates and executive situation-report format.

61–90 DAYS | Validate dependencies

Confirm recovery priorities, backup access, insurer requirements, counsel arrangements and critical supplier contacts.

91–120 DAYS | Exercise leadership

Run a realistic tabletop scenario that forces difficult containment, disclosure, recovery and stakeholder decisions.

121–180 DAYS | Close gaps

Remediate exercise findings, update plans and establish recurring executive and board exercises.

Executive Checklist

- ☐ Incident severity and escalation criteria approved
- ☐ Executive and technical incident leaders designated
- ☐ 24/7 contact and secure communications procedures tested
- ☐ Critical business services and recovery priorities documented
- ☐ External counsel, forensic and crisis advisers identified
- ☐ Cyber insurance notification requirements understood
- ☐ Regulatory and contractual notification pathways mapped
- ☐ Decision log and situation-report templates prepared
- ☐ Executive tabletop exercise completed within 12 months
- ☐ After-action findings tracked to accountable owners

Yakamichi Perspective

A cyber crisis compresses time, increases uncertainty and magnifies weak governance. The organizations that respond best are not those with the thickest incident manuals. They are those whose leaders have already practiced how to decide.

Executive incident readiness turns technical response into coordinated enterprise action, protecting critical operations while preserving legal, strategic and reputational options.

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