Establishing a Cyber BCP Framework in Response to Recent Major Hacking Incidents

---

1. Introduction

Recent large-scale hacking incidents at SKT, YES24, and SGI Seoul Guarantee have revealed significant vulnerabilities in Korea's ICT infrastructure and services. These events highlight the need for systematic response frameworks that go beyond incident management and move toward **Cyber Business Continuity Planning (Cyber BCP)**. This report analyzes major cases, interprets them from a BCP perspective, and proposes actionable approaches for Cyber BCP implementation.

---

2. Analysis of Major Hacking Incidents

2.1 SKT Hacking Incident

- Incident developed over two months, from system anomaly detection to public apology.
- Issues included delayed legal reporting, late response in SIM card replacement, and poor media handling.
- The incident escalated to government investigations and parliamentary hearings, significantly damaging corporate trust.

2.2 YES24 Hacking Incident

- Initial denial of hacking undermined credibility.
- Ransomware disclosure led to prolonged service disruptions and uncertainty over data breaches.
- Manual recovery efforts, repeated service outages, and ransom payments exposed severe BCP gaps.

2.3 SGI Seoul Guarantee Incident

- System outages disrupted electronic guarantee services and customer transactions.
- External support from financial and security agencies facilitated recovery.
- The incident showed reliance on external resources and highlighted the need for stronger internal BCP mechanisms.

---

3. BCP Perspective on Incident Response

- **T-1 (Prevention):** Threat detection and monitoring.
- **T0 (Incident Occurrence):** Damage assessment and emergency declaration.

- **T+1 (Emergency Response):** Containment and focus on halting escalation.
- **T+2 (Recovery):** Business relocation, alternative protocols, stakeholder communication.
- **T+3 (Normalization):** Full recovery, lessons learned, and prevention strategies.

Findings show weak **T0–T+1 response readiness** and insufficient **T+2–T+3 recovery structures** in domestic organizations.

---

4. Current Cyber Incident Trends

- Industry: Information & communications and manufacturing report the most incidents.
- Attack Types: Server hacking dominates, followed by malware/ransomware and DDoS attacks.
- Implication: Traditional BCP is inadequate against cyber-specific threats, emphasizing the need for Cyber BCP.

---

5. Cyber BCP: Concept and Importance

- **Definition:** A plan to minimize damages from cyberattacks and restore critical business operations within target recovery times.
- **Paradigm Shift:** Expands from recovery to prevention, deterrence, and resilience.
- **Global Trends:** The U.S., U.K., and EU are advancing cyber resilience policies; the EU is legislating the **Cyber Resilience Act**.

---

6. Comparison: Traditional BCP vs Cyber BCP

Category	Traditional BCP	Cyber BCP
Risk Factors	Natural disasters, power outages, pandemics, etc.	Ransomware, APTs, data breaches, DDoS, cloud outages, insider threats
Lead Department	CRO-led	CISO-led
Main Content	Physical recovery, workforce substitution, supply chain continuity	IT infrastructure recovery, data backup, cyber incident response, digital service continuity
Key Stakeholders	CEO, COO, CIO, HR, Finance, Legal, etc.	CISO, CTO, SOC, IT Ops, Security Vendors, Regulators

Cyber BCP requires **more agile, technology-driven responses** than traditional BCP.

---

7. Framework for Cyber BCP Implementation

1. **Capability Assessment**
   - Conduct third-party evaluations of policies, infrastructure, and workforce readiness.
2. **Simulation Exercises**
   - Test protocols for detection, assessment, emergency team activation, and communications.
3. **Framework Establishment**
   - Perform risk assessment and business impact analysis.
   - Build governance structures, response strategies, and recovery roadmaps.
   - Enhance through continuous training and iterative improvement.
4. **IT System Development**
   - Digitize response plans.
   - Automate task allocation, monitoring, and reporting.
   - Implement real-time alerts and compliance reporting functions.

---

8. Conclusion

These hacking cases demonstrate that cyber incidents are not only security concerns but also **existential risks for businesses and national trust**. Traditional BCP cannot adequately address cyber threats; a specialized **Cyber BCP framework** is essential.

Organizations must strengthen **proactive prevention**, build **resilient recovery mechanisms**, and ensure **continuous testing and training** to guarantee true business continuity in the cyber era.

Would you like me to expand this into a **full professional report format** (with cover page, table of contents, and executive summary), so it can be used directly for presentations or submissions?