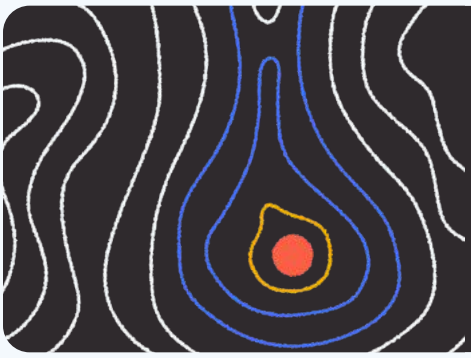
THE IMPORTANCE OF CYBER RESILIENCY IN MODERN THREAT LANDSCAPES

This white paper highlights the critical role of cyber resiliency in safeguarding organizations. Cyber resiliency ensures that businesses can withstand, respond to, and recover from cyber incidents. We explore how assessments, detection, prevention, and recovery work together to build resilient organizations, and how Koniag Cyber enables success through comprehensive services and solutions.

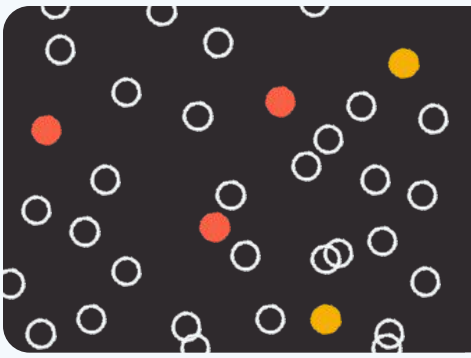
With the growing sophistication of cyber threats, resiliency is no longer optional—it is the backbone of modern cybersecurity strategies. While prevention and detection remain essential, organizations must also prepare to withstand and recover from inevitable incidents. Cyber resiliency ensures business continuity, protects stakeholder trust, and secures long-term operational stability.

The Pillars of Cyber Resiliency



Assessment

Regular risk assessments are foundational to building resiliency. They identify vulnerabilities, misconfigurations, and gaps in existing defenses. Effective assessments help organizations prioritize security investments and align risk management efforts with business goals. Koniag Cyber provides tailored assessment services that benchmark current capabilities and develop actionable improvement roadmaps.



Detection

Detection capabilities allow organizations to swiftly identify abnormal or malicious activity before it escalates. Continuous monitoring, threat hunting, and anomaly detection are core elements of a resilient cyber strategy. Koniag Cyber leverages advanced SIEM tools, endpoint detection and response (EDR), and behavioral analytics to ensure rapid threat identification and containment.

Prevention

Prevention encompasses the proactive measures taken to minimize attack surfaces and block threat actors before they can do harm. This includes the use of Zero Trust Architecture, strict access controls, vulnerability management, encryption, and employee awareness training. Koniag Cyber's prevention solutions help clients stay one step ahead by reducing risk exposure and enforcing layered defenses.

Recovery

Even the most secure organizations can experience incidents. Recovery is a critical component of resiliency that ensures operations can continue and return to normal quickly after a breach or disruption.

Our team treats recovery not as a last resort, but as a strategic priority. By integrating recovery into every stage of our cybersecurity lifecycle, we help organizations build a culture of preparedness and resilience—capable of withstanding and bouncing back from even the most severe cyber events.

Key Elements of Recovery

Data Backups
Consistent, automated backups of critical systems and data allow for swift restoration. Koniag Cyber designs backup strategies that support both rapid recovery and long-term data integrity.

Business Continuity Planning (BCP)
Beyond IT systems, BCP ensures that essential business operations can proceed despite disruptions. Koniag Cyber supports organizations in mapping out continuity procedures for critical departments and personnel.

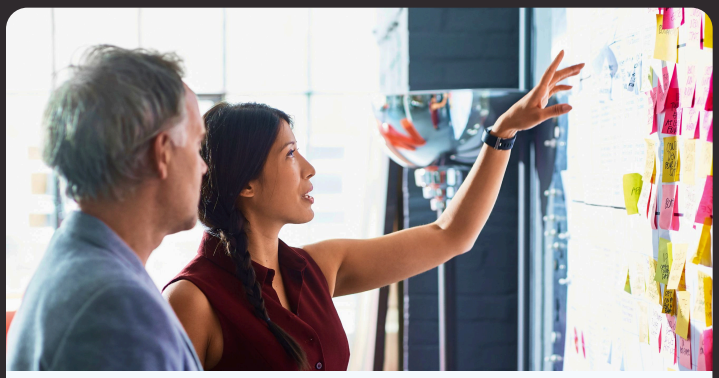
Disaster Recovery Planning (DRP)
A detailed DRP outlines actions to restore systems and applications following an incident. We help organizations develop, test, and refine DRPs that meet regulatory, technical, and operational requirements.

Recovery Testing
Recovery plans must be actionable under pressure. We facilitate recovery exercises, scenario planning, and simulations to ensure that plans are realistic and personnel are confident in their execution.

The Koniag Cyber Advantage

Koniag Cyber offers a full-spectrum approach to cyber resiliency that integrates all four pillars: **assessment**, **detection**, **prevention**, and **recovery**. Our solutions are customized to each client's environment, regulatory landscape, and mission priorities. Together, we bring decades of experience supporting both commercial and federal clients with mission-critical cybersecurity and resiliency initiatives.

What sets us apart is the strength of the **Koniag family of companies**, which includes:



vervint.

Vervint, a technology consulting firm serving commercial enterprises

Koniag Government Services

Koniag Government Services (KGS), a trusted partner to federal agencies

Why it matters to your business and your people:

Maintain High Trust

Cyber Resiliency helps you mitigate outages. Nothing erodes trust faster with clients and partners than a cyber-induced disruption. Maintain the trust you've earned.

Invest Now, Save Big Later

Breaches can cost millions of dollars in downtime, fines, or ransomware payments. Invest, and do all you can to avoid becoming a victim later.

Keep Critical Services On

Humans rely on you. Your cyber preparedness can help keep critical services operational, and that can save lives.

Cyber resiliency is no longer a luxury—it's a necessity. In an era of advanced threats and rising risk, organizations must go beyond defense and build systems that **withstand, adapt, and recover**. By combining assessment, detection, prevention, and recovery, Koniag Cyber empowers clients to navigate cyber adversity with confidence and continuity.