kyndryl

Kyndryl Security and Resiliency for the US public sector

The US public sector continually faces unique challenges that threaten its ability to operate.

The public sector in the United States underwent rapid digital transformation during the COVID-19 pandemic, enabling and enhancing services for constituents while also leading to new and emerging threats that range from major supply chain issues and inflationary concerns to being targeted in a cyber war.

To best serve their communities, public sector leaders are quickly realizing they need to implement guardrails for resilience in a constantly changing threat landscape.

There are three main threats leaders are preparing for in order to remain resilient:

Cyber threats

Every day, new headlines emerge about government agencies forced to cease operations because their IT systems have been compromised by a cyberattack. The shift to serving communities remotely has only amplified the impact when those shutdowns occur. Lower barriers to entry for cyberthreat actors, more aggressive attack methods, a shortage of cybersecurity professionals, and patchwork governance mechanisms are all aggravating the cyber risk.

Cyberattacks are also becoming more sophisticated, increasingly carried out by nation- or state-sponsored threat actors.[4] In 2020, a group suspected of being backed by the Russian government penetrated thousands of organizations around the world—including multiple parts of the US federal government, which led to a series of data breaches. This cyberattack and subsequent data breach affected over 200 organizations, including NATO, the UK government, and European Parliament, and is reported to be among the worst cyber-espionage incidents the US has ever suffered.

Rising IT complexity
The pandemic forced the US government to undergo rapid digital transform, enabling remote workers and shifting applications to the cloud. Though it greatly enhanced the ability to serve their communities remotely, that rapid transformation caused some growing pains and created an increasingly complex IT environment vulnerable to both cyberattacks and IT outages—for example, a phishing attack that targets a government employee's computer could infect critical processes due to the interconnection between systems.

Extreme weather events
Extreme weather was ranked by global leaders in a World Economic Forum survey as the top short-term risk to the world.[5] In the US, we constantly see how governments are forced to quickly adapt to new extreme weather events—things that have never had to deal with in the past, including major snowstorms in traditionally warmer climates, droughts, heavy rainfall, and more. These changes are introducing an entirely new threat vector that may be unfamiliar to local leaders.

85%
Of organizations have been the victim of a successful cyberattack in the past 12 months[1]

+104%
Growth in ransomware attacks between 2020 and 2021[2]

$5M
Average cost of a ransomware attack[3]

How to ensure operational continuity

The US public sector can mitigate IT and operational risks across the threat spectrum by securing corporate applications and data, maintaining the highest availability of services, and remaining compliant with regulations.

Building resiliency requires organizations to focus not only on responding and restoring operations after a disruption has occurred, but also continuously expanding and optimizing with an emphasis on productivity and quick decision-making and accelerating and innovating through new growth opportunities in the wake of a disruptive event.

The Kyndryl approach

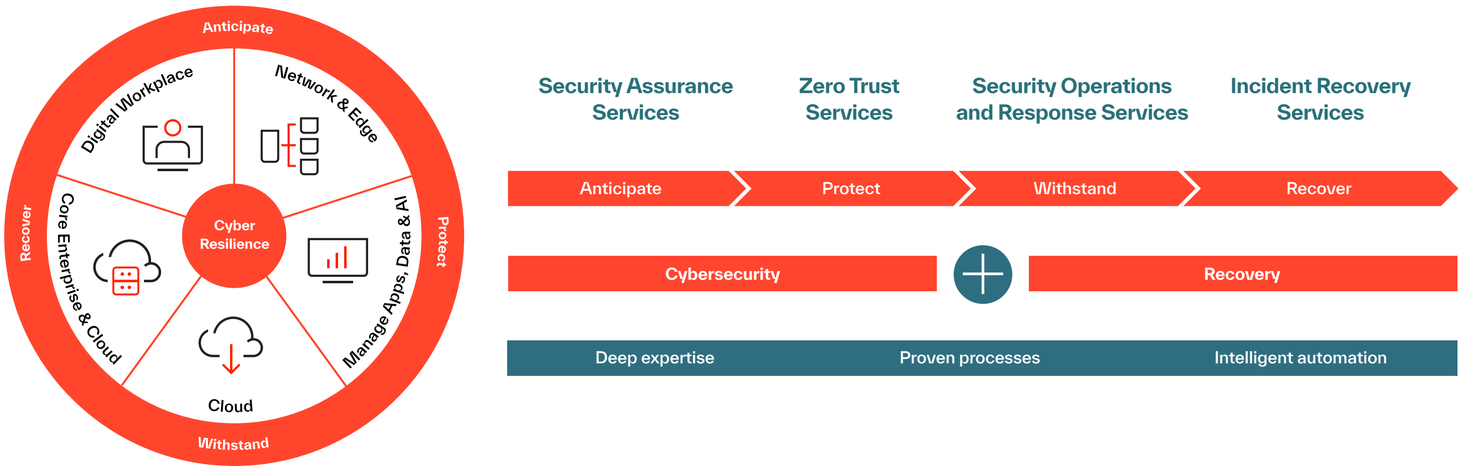
For governments, the need for resiliency isn't new. With every new disruption—from natural disasters and power outages to the growing threat of cyberattacks—public sector leaders find a way to keep operating and serving their communities.

Kyndryl believes in resiliency and continuity in the face of any threat. Government organizations need to go further than cybersecurity, driving toward cyber-resilience and designing for risks beyond our sphere of influence—especially when responsible for critical infrastructures.

"Why is cyber resiliency important? It's important because you can't stop cyberattacks. Even with the right safeguards and countermeasures in place, some attacks will be successful."

– Ron Ross, NIST Fellow[6]

Kyndryl cyber resilience framework



Our cyber resilience framework incorporates the National Institute of Standards and Technology (NIST) cybersecurity framework to assist in recoverability across the spectrum. Our approach is designed to ensure public sector organizations can anticipate, protect against, withstand, and recover from adverse conditions, stresses, attacks, and compromising threats.

The concept of cyber resilience is based on the assumption that adversaries will eventually breach even the best defenses—a question of when, not if—and these adversaries will establish a long-term presence through breaches or supply chain attacks. Cyber resilience must be provided in a cyber-contested environment that includes the Advanced Persistent Threat (APT).

When an organization is highly resilient, it can withstand cyberattacks, faults, and failures, continuing to operate and carry out vital business functions even in a degraded or debilitated state.

Kyndryl's cyber resilience framework is split into four areas:

1. Security Assurance Services

As the skills gap continues to widen, public sector organizations need a partner with deep expertise to help them assess operational and cyber risks and establish policies, controls, and compliance programs that are closely aligned with organizational objectives.

Our experts can help you assess and benchmark cybersecurity and resilience maturity, define your organization's target state, gain visibility into threats and exposures, and enable the consistent application of security policies and controls.

- **Security, strategy, and risk management:** Assess your organization's cyber resilience and data compliance posture, and benchmark industry standard security controls. Uncover hidden threats and vulnerabilities that could expose your organization to data breaches and take strategic measures to avoid damaging impacts.
- **Offensive security testing:** Gain visibility into significant threats and vulnerabilities across your network, use advanced attack simulation to identify, prioritize, respond to, and remediate real-world cyberattacks. Carry out process testing programs, including offensive security testing of hardware, devices, and networks, as well as penetration testing for IoT devices to find security loopholes.
- **Compliance management:** Ensure compliance with regulations and audit readiness through a security risk assessment based on NIST SP-800 and Europe's NIS Directive and quantify your potential financial exposure with our compliance management services.

2. Zero Trust Services

Kyndryl is a strong proponent of zero-trust security to dramatically improve an organization's cyber resilience posture. In auditing terms, zero trust should be considered a primary control—but we also need secondary controls.

> Office of Management and Budget (OMB) released a Federal strategy to move the U.S. Government toward a "zero trust" approach to cybersecurity. The growing threat of sophisticated cyber-attacks has underscored that the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. The Log4j vulnerability is the latest evidence that adversaries will continue to find new opportunities to get their foot in the door. The zero-trust strategy will enable agencies to more rapidly detect, isolate, and respond to these types of threats.
>
> – *White House Office of Management and Budget*[7]

With this in mind, we design our solutions for extreme, in-depth defense using a zero-trust model for optimal cyber resilience.

3. Security Operations and Response Services

Visibility is key to protecting your organization against the menace of advanced cyberattacks. As systems, tools, and applications are increasingly scattered in a hybrid environment—in the cloud and on premises—security operations teams often struggle with threat detection and response.

We'll help you harness the power of analytics and other emerging technologies to detect, triage, investigate, and respond to advanced cyberthreats before they impact your organization. Our security operations and response services leverage AI-powered threat detection and incident response to eliminate false positives, focus on threats that matter, and improve response times.

- **Advanced threat detection:** Stay a step ahead of detected and undetected cyberthreats and stop them in their tracks with 24/7 threat prevention, detection, and response capabilities powered by AI—all while improving the productivity of your security operations center. Protect devices across your environments and mitigate endpoint attacks with endpoint monitoring and management features.
- **Incident response and forensics:** Investigate and respond to a detected security incident with capabilities like incident triage, incident response, threat intelligence curation and management, and compliance monitoring their communities depend on.

4. Incident Recovery Services

Traditional disaster recovery planning and strategies are unable to keep up with changing cyber recovery requirements and may result in risk exposure to outages that cause irreparable damage.

Incident Recovery Services from Kyndryl use best practices, purpose-built technologies, and expertise to assess your incident response readiness and build an incident recovery plan aligned to your organizational needs. Our cyber resilience solutions are designed to mitigate the impact of an outage and provide fast, reliable, and scalable recovery across hybrid multicloud environments.

- **Cyber incident recovery:** Mitigate the impact of cyber disruption with an orchestrated resilience approach that helps identify risks, protect data and applications, and rapidly recover IT.
- **Managed backup services:** Minimize the risk of data loss with our fully managed data backup services that provide access to your information—anytime, anywhere—and help you protect and retrieve critical data quickly after a cyber incident. Flexibly scale your backup data volume according to your organization needs, and support information resiliency using analytics to monitor the health of your data protection environment.
- **Hybrid platform recovery:** Reduce risk to systems, facilities, and data and recover your organization from a disaster. Our automated recovery capability enables rapid failover and failback for your computing environments across physical, virtual, cloud, and traditional layers, with cloud landing zones for failover to help you achieve improved agility, flexibility, and cost efficiency.
- **Data center design and facilities:** We'll help you design, build, and manage optimized, cost-effective data centers and facilities to achieve lean, resilient, flexible infrastructure. Get the flexibility you need to support future technology and computing model adoption and accommodate a mix of hosted services across environments. Drive greater efficiency by identifying equipment for technology refresh and improving visibility into the consolidation and virtualization of your data center.
- **Recovery retainer:** Get experts on the ground to help you recover from a cyber incident, available remotely or onsite upon notification of a cyber incident. Kyndryl offers three recovery retainer tiers, all of which include an intake workshop, access to 24/7 phone support, and a predefined number of hours for our experts to support your recovery requirements in the event of a disruptive cyber incident, such as a ransomware attack.

In a digital world, cyber resilience must be a component of any public sector organization's planning, be it new lines, new applications, or new units. Cyberattacks will only increase, but organizations can build resiliency in the face of attacks by investing in a comprehensive strategy to reduce downtime, decrease long-standing damage, and, most importantly, continue to deliver the uninterrupted services their communities depend on.

Why Kyndryl?

Kyndryl has been a thought leader in the business continuity world since the 1960s. Cybersecurity and resilience are in the DNA of Kyndryl, where we work.

55+

Years of business continuity and disaster recovery experience.

10K

Customers protected

380+

Datacenters operated in 70 countries, covering 8M+ sq feet

3.6

Exabytes of customer data managed

6K+

Professionals dedicated to business continuity.

100%

Success in meeting commitments to customers who declared incidents

Cyber resilience design methodology

Kyndryl can bring its cyber resilience methodology to dramatically improve the recoverability of your most critical processes.

Ask yourself:

- If our IT systems go down, how am I going to track inventory, manage accounts, or communicate with offices and plants?
- Are we able to measure and predict the amount of time we expect to be down from a cyber-attack (cyber-RTO) and the amount of data we expect to lose from a cyber-attack (cyber-RPO)?

Kyndryl's cyber resilience model was built over decades in the business continuity world, compiled from hundreds of sources including our own analysts, industry analysts, backup and disaster recovery software vendors, regulatory agencies around the world, and military doctrine derived from NSA, NIST, and US Cyber Command.

Our methodologies start with assessments, Kyndryl recommendations, scoring, and professional deliverables. Whether you're looking at an application, unit, process, data center, or cloud journey, let's work together to co-create a zero-trust cyber resilience design and strategy that works for your organization's unique requirements.

Zero-trust design methodology

Our zero-trust design methodology borrows from major vendors, analysts, and government standards bodies, including Google, Gartner, Forrester, and NIST. We can help you advance your zero-trust journey with any type of use case, from individual application migrations to entire data center cloud migration.

Kyndryl recovery retainer

Unlike many existing incident recovery retainers, our recovery retainer service can assess an organization's existing cyber resilience posture and run recovery actions remotely or onsite, enabling organizations to quickly recover their production environment and return to operations.

- Proactively strengthen cyber incident recovery preparedness and plan for response
- Reduce the impact of cyber incidents
- Overcome skills shortage with on-demand availability of cyber recovery experts

Why Now?

Historically, funding has been a barrier to modernization initiatives. With the Infrastructure Investment and Job Act (IIJA) and more than USD $1.6B allocated specifically for cybersecurity programs, federal, state, and local governments have an opportunity to invest in the technologies needed to digitize government services, bolster cybersecurity and resiliency, and modernize US infrastructure. We have established the Kyndryl Public Sector Grants Program to help you unlock funding from ARPA and IIJA.

kyndryl

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

[1] *2022 Cyberthreat Defense Report*, CyberEdge Group, 2022

[2] *Cyber Threat Report 2022: Mid-Year Update*, SonicWall, 2022

[3] Estimate based on: *Cost of a Data Breach Report 2022*, IBM, July 2022

[4] *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*, Harvard Business Review, February 2022

[5] *The Global Risks Report 2022*, World Economic Forum, 2022

[6] *NIST Updates Cyber Resiliency Guidance for Critical Systems*, Ron Ross, August 2021

[7] *Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture*, White House press release, January 2022