Protect federal, state, and local governments from third party-related cyberattacks

Lower your risk with AI and automation

No government organization is immune from third-party risk

Cyberattacks have become so common we are almost numb to the news headlines. A 2020 study found **third-party breaches jumped 35 percent** from 2017 to 2019, and the quantity of records exposed shot up 273 percent from 2018 to 2019, averaging 13 million records by 2019.[1] Perpetrators often use an organization's third parties as points of entry to conduct these cyberattacks. On Christmas day 2020, a breach through third-party file transfer software exposed personal information of 1.6 million Washington state employees and residents who filed for unemployment in 2020.[2] We all know about the SolarWinds breach that affected U.S. Departments of Treasury, Commerce, and Homeland Security via legitimate third-party software updates.[3]

Government organizations, citizens, and employees reap uncountable benefits from digital transformation, but these benefits can come with risk. Only 48 percent of government leaders surveyed use cybersecurity technologies and services to enable their organization's digital transformation.[4] Organizations rely on third-party tools to add new digital capabilities. Sometimes these tools open a door to allow cyberattacks. Threats are more frequent and breaches are larger in scope making it a priority for federal, state, and local governments to **tighten third-party selection due diligence processes**. This article covers methods that **use automation and artificial intelligence (AI) to lower risk of attacks** via third parties.

Why modern government is important

Government agencies in the U.S. must modernize in order to keep up with changing user needs, regulations, and health and public safety requirements. Leaders of modern governments rethink business processes and service delivery models to more effectively achieve their mission. This article is one of a series that features how modernizing affects the government workforce and the user experience, improves security and public trust, and accelerates the digital journey. KPMG team members offer insights intended to help guide governments in their modernization efforts to encompass all processes, technologies, policies, and the workforce so each works together to create connected, powered, and trusted organizations.

[1] Jai Vijayan, "Third-party breaches – and the number of records exposed – increased sharply in 2019," Dark Reading, February 12, 2020.

[2] Nicole Jennings, "WA Auditor's Office: No information 'misused' so far in Accellion breach," MYNorthwest, June 16, 2021.

[3] Sophie Bushwick, "Giant U.S. Computer Security Breach Exploited Very Common Software," Scientific American, December 15, 2020.

[4] "Impacts of COVID-19 on digital transformation strategies and the future of work," KPMG and Forrester, 2020.

Knowledge is power to prevent third-party-related breaches

Ignorance is not a defense. What government leaders and team members do not know about **third parties** can have a deep and negative impact to their organization. Federal and state mandates require that government organizations appropriately manage and protect their own information as well as data for which they are stewards. At the federal level, these **mandates extend to any third-party product or service**.

The federal government has a new executive order that lays out its plan to improve the nation's cybersecurity, including steps agencies must take. **Third parties supporting federal government agencies will have to meet requirements** including cybersecurity incident reporting, cloud security principles, software standards, network logs, and using data encryption and multifactor authentication.[5] The Department of Defense requires vendors, contractors, and subcontractors to meet Cybersecurity Maturity Model Certification requirements.[6]

Some **states are lowering their risk exposure** after constant cyber threats across the industry. For example, Pennsylvania is updating its Breach of Personal Information Act following a data breach that exposed health records for 72,000 people in Pennsylvania. The state terminated the contract because the third-party vendor was not transparent regarding the breach.[7]

With or without laws or regulations, every government organization needs an active **third-party risk management strategy and program** to evaluate and monitor for risks before, during, and after contracts are in place. We recommend the following critical steps:

1. **Program development:** Define and implement, or evaluate and enhance, your third-party risk management program. Segment third parties by which are critical and potentially high risk. Identify which vendors have access to your organization's critical data, where they store your data, and how they protect it.

2. **Third-party assessments:** Evaluate how continuous controls monitoring can align with program goals rather than using standard inherent risk questionnaires, due diligence, assessments, and on-site reviews. Consider whether point-in-time assessments are still valuable.

3. **Control monitoring:** Identify continuous controls monitoring up front. Rethink how the combination of data-driven, proactive risk monitoring with AI and machine learning can enable early warnings for third-party resilience and help mitigate risk.

4. **Risk reduction and failed control remediation:** Address third-party contractual security, operational requirements, and risk remediation.

[5] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.

[6] Matthew Hodson, "Increased Cybersecurity Mandates Coming for State and Local Governments," Security Magazine, June 11, 2021.

[7] Lindsay Ward, "Pa. Senate holding Hearing Over COVID-19 Contact Tracing Data Breach," KDKA C2 CBS Pittsburgh," May 24, 2021.

Third-party risk management can be proactive with automation and AI

Cybersecurity threats will likely not subside, especially considering government organizations' growing reliance on third parties. This means federal, state, and local governments must depend on effective **third-party risk management to stay ahead of the intensifying threats**.

KPMG works with government clients using a risk-based approach that provides intelligence to help proactively manage third parties and mitigate risk. The technology-agnostic approach uses AI analytics and engineering as well as AI principles across the third-party security process lifecycle. AI and automation enhance the ability to **identify, evaluate, and respond to threats**. Our method helps organizations:

- **Connect enterprise applications and data** such as contract management and procurement with a user-friendly front end as a holistic interface between operations, security, compliance, and the third party.
- **Manage risk** using advanced analytics and standard third-party assessments:
  - Our third-party security program assessment and benchmarking service uses standards and security models. These help organizations assess third-party security readiness against peer organizations and recommend improvements.
  - Users can test security program components in our third-party security lab's interactive simulation.
  - Our team helps streamline and automate processes. They use an assessment framework that runs large-scale third-party security assessments in a smarter way and helps organization leaders realize the value of the managed service.
- **Use automation and AI** to automate less complex tasks such as managing security assessments and add intelligence about each third party, their behaviors, and when they perform actions outside of approved services. Machine learning picks up behaviors from human interaction and also verifies and correlates data in real-time against the organization's tolerance levels.
- **Track contracts** with visibility into security provisions and data sharing included in them.
- **Gain visibility into third-party environments** across regions, languages, and assessors. Clients have near-real-time visibility into their third parties' security posture with continuous monitoring and assessment that enables a risk remediation culture.
- **Accelerate digital transformation** as a solution framework that delivers, teaches, and elevates organizations to move from a human-powered cyber workforce to a human-accelerated, AI-enabled organization.

Our third-party risk management approach includes these steps and outcomes:

Identify	Assess	Evaluate	Recommend	Integrate	Communicate
Rationalize third-party database; eliminate duplicate entries	Fast-track assessments and identify priorities and changes in approved services	Present a holistic third-party view across assessors and departments	Predict and challenge inherent, residual risks based on historical data	Connect enterprise applications for big-picture visibility	Deliver consistent, automated messaging across channels and departments

Federal, state, and local governments are all targets, and the rise in remote working adds significant risk. More than half of the 3,000 workers who responded to a recent survey said they had used their work devices for personal online banking and over one-third had connected to smart devices such as speakers.[8] Thorough **assessments and continuous monitoring** powered by **automation and AI-powered third-party risk management is the best defense**.

Better cybersecurity can improve trust. One study found 64 percent of Americans do not trust federal agencies with their personal information.[9] This response is not a surprise since federal governments are usually larger targets. For example, in June, hackers hit the third-party vendor that provides email newsletter services to the U.S. House with a ransomware attack.[10]

Some state and local governments are boosting their cybersecurity legislation and activities to prevent data breaches and ransomware.[11] A ransomware group claimed responsibility for a St. Clair County in Illinois attack in May that shut down all online services for residents and county workers.[12] The same hackers are believed to be responsible for a similar attack on a Washington school district. As a result of the malware attack, student photos and performance results showed up on the dark web.

The results of security assessments with continuous monitoring can offer government leaders a **comprehensive, real-time view of their third parties' readiness** to prevent, detect, contain, and respond to information security threats such as these. Whether an organization is developing or building a program or starting to explore AI and machine learning to enhance it, KPMG third-party risk management government professionals can help.

Outsmart the hackers with indestructible third-party risk management

In a world that becomes more digital each day, risks that your organization will be hit with a cyberattack grow exponentially, and odds are the attack will involve a third party. Companies and organizations across all industries, including government, seek to lower risk by performing due diligence on any third-party company with whom they work. You have the power to save your federal, state, or local organization time, money, and reputation by better managing third-party risk across operations.

[8] James Rundle, "Why the Hybrid Workplace is a Cybersecurity Nightmare," The Wall Street Journal, June 9, 2021.

[9] "How privacy-enhancing technologies can ease customers' confidentiality concerns," PYMNTS.com, June 17, 2021.

[10] Erik Wasson, Billy House, "U.S. House Email system Vendor hit with Ransomware Attack," Bloomberg, June 8, 2021.

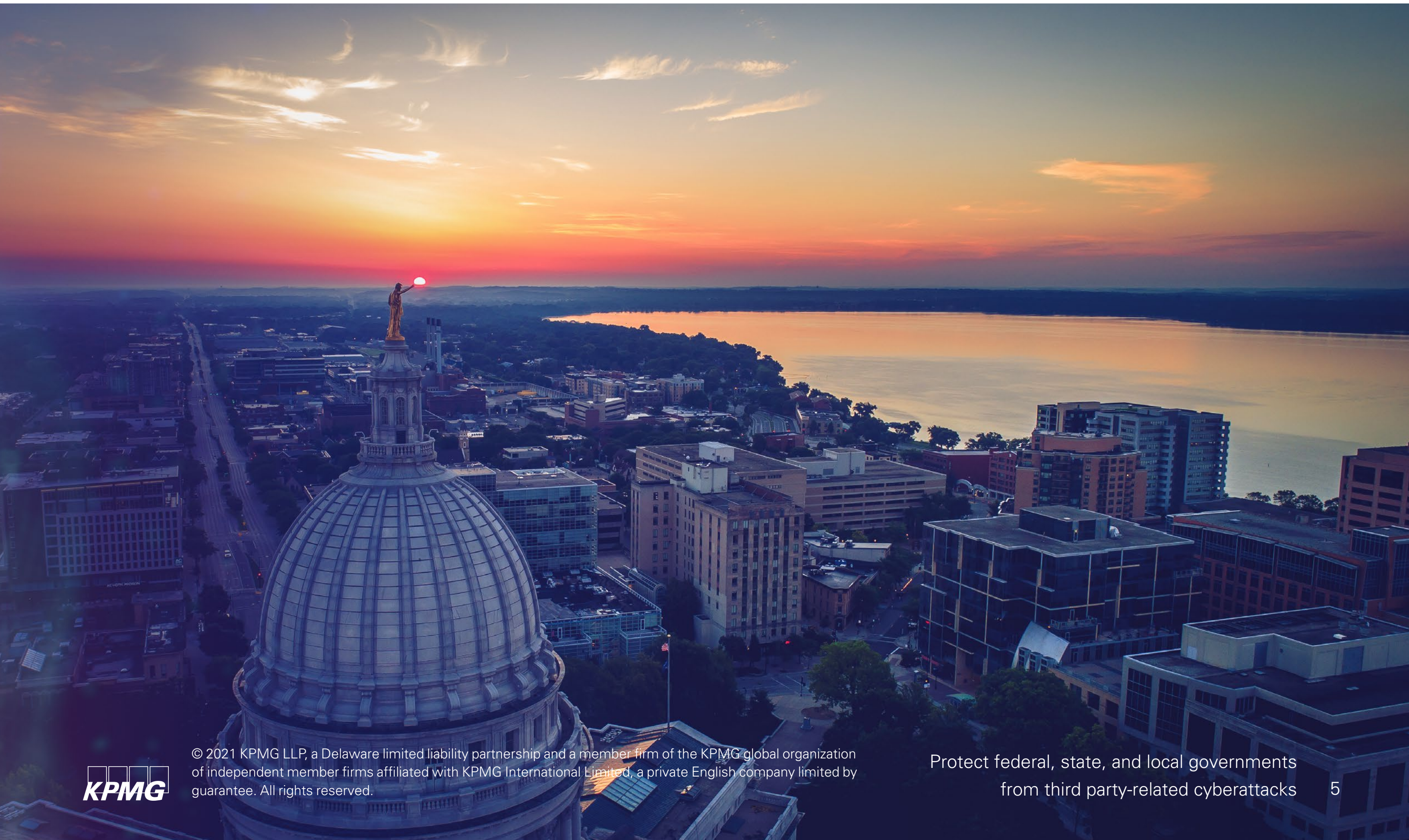
[11] Matthew Hodson, "Increased Cybersecurity Mandates Coming for State and Local Governments," Security Magazine, June 11, 2021.

[12] Andy Banker, "St. Clair County victimized in ransomware attack," Fox2 Now, June 3, 2021.

About KPMG

KPMG has worked with federal, state, and local governments for more than a century, so we know how agencies work. Our team understands the unique issues, pressures, and challenges you encounter in the journey to modernize. We draw on our government operations knowledge to offer methodologies tailored to help you overcome these challenges and work with you from beginning to end to deliver the results that matter.

The KPMG team starts with the business issue before we determine the solution because we understand the ultimate mission. When the way people work changes, our team brings the leading training practices to make sure your employees have the right knowledge and skills. We also help your people get value out of technology while also assisting with cloud, advanced analytics, intelligent automation, and cybersecurity. Our passion is to create value, inspire trust, and help government clients deliver better experiences to workers, citizens, and communities.



Contact us

Tony Hubbard

Principal, Government Cyber Security Leader
KPMG LLP
202-486-4945
thubbard@kpmg.com

Joseph Klimavicz

Managing Director, Federal CIO Advisory Leader
KPMG LLP
703-795-8999
jklimavicz@kpmg.com

Kathy Cruz

Director, Government Cyber Security Practice
KPMG LLP
916-792-3976
kathycruz@kpmg.com

read.kpmg.us/modgov

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.