PRESIDIO FEDERAL

IBM Gold Partner

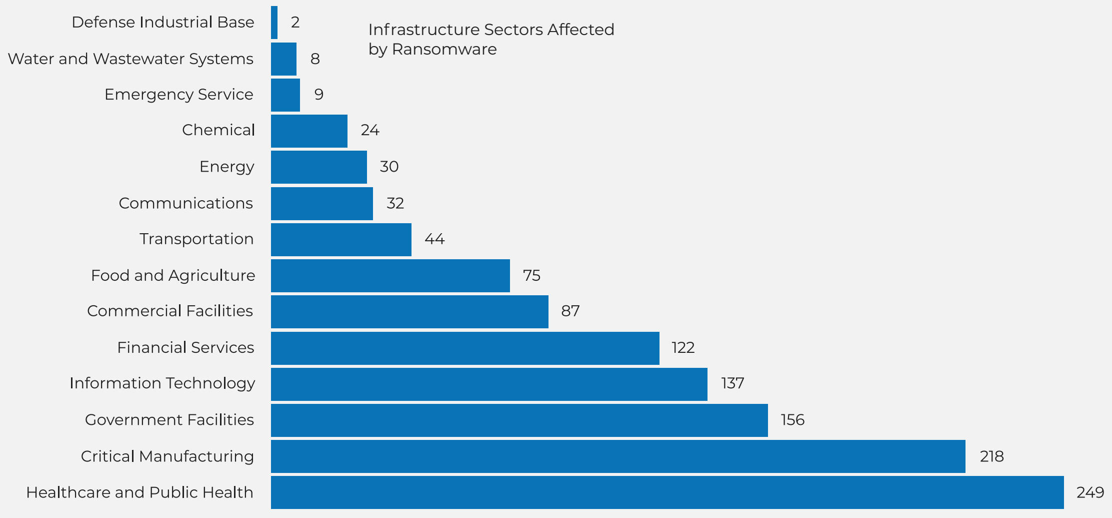
Navigating AI's role in mitigating ransomware threats

Cyberthreats against the federal government are increasing. In 2023, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) received 880,418 complaints, which was up nearly 80,000 from 2022 numbers and accounting for $12.5 billion in adjusted losses. Of these complaints, "2,825 complaints were identified as ransomware with adjusted losses of more than $59.6 million."

In the FBI's 2023 Internet Crime Report, the IC3 identified three sectors as popular targets for cybercriminals: health care, critical manufacturing and government facilities. While health care led the way with 249 reports of ransomware, government facilities weren't far behind with a total of 156 reports in 2023.

With threat actors increasingly looking to disrupt, deny and disable normal operations, any interruption or downtime could cause severe consequences, as witnessed during the Colonial Pipeline ransomware attack. On May 7, 2021, DarkSide, a cybercriminal group, managed to infiltrate Colonial Pipeline's network and encrypt hundreds of gigabytes of data, leading to the eventual shutdown of Colonial's network. Eventually, service was restored to the network, but not before the general public in 18 states struggled with skyrocketing fuel prices and empty gas pumps.

After the Colonial Pipeline ransomware attack, it became apparent that a "whole-of-nation" approach to cybersecurity would be required to effectively protect against emerging threats. This means the federal government and private sector must work together to protect data and keep protections at pace with advancing adversaries.Indeed, attacks are becoming more sophisticated. For example, according to an article published by the MIT Sloan Management Review, entitled From ChatGPT to HackGPT: Meeting the Cybersecurity Threat of Generative AI, threat



actors are weaponizing generative artificial intelligence (AI) to improve existing strains of ransomware and malware, as well as to scale-up phishing attacks.

Given the increasing sophistication of these attacks, now is the time for federal facilities to invest in next-generation capabilities to stay ahead of tomorrow's threats.

"Protecting federal data from exploitation is no easy task," Jon S Kim, VP of Solutions and Services at Presidio Federal said. "Threat actors are increasingly using contemporary technology to circumvent traditional security backstops, but federal agencies can use tools like generative AI and machine learning (ML) to detect, prevent and respond to threats in real time."

Protecting mission data at scale

Effectively responding to ransomware starts with the ability to detect ransomware in backups.
Teams at federal agencies must be able to detect and determine if a previous version is corrupt. Often, this requires organizational leadership to pull employees or resources from other projects, leading to costly delays.

Ultimately, legacy systems are vulnerable and organizations across the federal government require solutions that can help them defend against ransomware before their data is under attack.

"Generative AI could help the federal government protect their data from threat actors, but any tool set in place must meet rigorous ethical standards and be safe-by-design. Decision-makers need solutions and capabilities that rise to meet ever-evolving demands and can deliver at the speed and scale of the mission at hand," Kim said.

Through IBM, agencies can achieve this by ensuring all systems designed, built and deployed adhere to the following quality standards:

Explainability — Algorithmic decisions should be clear, concise and easy to understand. Systems should provide context around how the system came to a certain decision.

Fairness — AI systems should not be making decisions alone. Human-machine teaming is critical to addressing any potential biases that may be present in any decision.

Robustness — AI systems should be built to defend against intentional and unintentional interference.

Transparency — Users should be able to understand how the system works, its capabilities and its limitations. AI systems should not be a complex "black box" where decisions are made, it should be easy to follow the algorithm's decision-making.

IBM's Storage Defender — an AI-informed data resiliency solution designed to help federal facilities recover from data loss by integrating immutable backups — is built with these pillars in mind so that federal agencies can effectively recover from ransomware faster. However, the federal government cannot and should not invest blindly. In her remarks to Carnegie Mellon University on February 27, 2023, Cyber and Infrastructure Security Agency Director Jen Easterly emphasized that unsafe products could jeopardize progress.

"While a focus on adversary nations — like China and Russia — and on cybercriminals is important, I would submit to you that these cyber-intrusions are a symptom, rather than a cause, of the vulnerability we face as a nation. The cause, simply put, is unsafe technology products. And because the damage caused by these unsafe products is distributed and spread over time, the impact is much more difficult to measure," Easterly said.

Presidio Federal and IBM recognize the need for secure-by-design solutions and have been working toward radically transparent offerings built to meet today's mission needs.

Together, they are actively working toward the creation and deployment of solutions that meet Easterly's call for secure-by-design solutions. IBM's AI Ethics Framework, Board and Pillars all inform how strategic partners need to design, build and deploy systems. Transparency, accountability and clarity are the bedrock of how we move forward as a nation, and how we protect user information from exploitation.

Securing data starts with close collaboration.
Together, Presidio Federal and IBM, are leaders in their field with decades of experience serving the public sector and delivering contemporary solutions designed with the mission at the forefront.

> "We're actively working toward the creation and deployment of solutions that meet Easterly's call for secure-by-design solutions. "
>
> Jon S Kim, VP of Solutions and Services at Presidio Federal

And as threats continue to evolve, Presidio Federal and IBM are investing in sustainable cybersecurity efforts as a way to move the dial and proactively combat ransomware.

"A sustainable cybersecurity model is the only way we can move forward as a nation, protecting critical data is the job of everyone. At Presidio Federal and IBM, we've incorporated these tenets into our day-to-day operations, we're dedicated to building solutions that are not only transparent, but we're dedicated to working with our customers to offer secure-by-default solutions designed to protect information at rest and in motion," Kim said.

Visit **www.presidiofederal.com/partners/IBM** to learn more about how IBM and Presidio Federal are secure, sustainable cybersecurity practices.