In a rapidly evolving digital world, the importance of strong cybersecurity cannot be overstated. The Infrastructure Investment and Jobs Act (IIJA), also known as the Bipartisan Infrastructure Law (BIL), includes provisions to bolster cybersecurity across several sectors.

The path to a more secure digital world

Here are a few ways that IIJA’s funding can enhance your cybersecurity:

1. **Strategic cyber governance and planning:** Create clear cybersecurity policies and incident response plans, ensuring a coordinated approach to digital security.
2. **Mitigating prioritized issues:** Address critical cybersecurity issues by allocating resources to tackle vulnerabilities and threats with the highest risk.
3. **Assessing and evaluating systems and capabilities:** Enable comprehensive audits of systems, hardware and software to identify vulnerabilities and weaknesses.
4. **Building a cybersecurity workforce:** Support the development of a skilled cybersecurity workforce through training and education programs.

Enhance your cybersecurity posture against data breaches.

**Verizon**’s Trust Center will help you:

- **Leverage Internet of Things (IoT) technologies to protect your linked devices and remote workers.**
- **Strengthen telecommunications and industrial controls against hacking.**
- **Leverage Verizon’s endpoint security and professional services encompasses managed detection and response, network detection and response, and cybersecurity incident response.**

**The IIJA is a critical resource to help you address these challenges.**

Find out how Verizon’s cybersecurity solutions can help future-proof your organization.

**$1.82 million** is the estimated average cost to recover from a ransomware attack.4

Verizon’s Zero Trust Dynamic Access and Secure Access Service Edge (SASE) Management can play a pivotal role in bolstering cybersecurity defenses for users, apps and data on devices while maintaining day-to-day operations.

**62%** of companies experienced a security breach that could be at least partially attributed to an employee working remotely.5

**83%** of breaches noted in Verizon's 2023 Data Breach Investigations Report data were caused by external actors, such as criminal groups and hacktivists.

**In 2023, 69%** of state and local governments were hit by ransomware attacks, up from **58%** in 2022.2

**51%** of organizations are planning to increase security investments as a result of a breach.3

**6%** of state and local government information technology staff are responsible for cybersecurity and IT vulnerabilities, a direct result of a lack of cybersecurity skills.

**62%** of state and local government IT managers said they are responsible for cybersecurity and IT vulnerabilities, a direct result of a lack of cybersecurity skills.

**51%** of organizations are planning to increase security investments as a result of a breach.3

**69%** of state officials are concerned about the extent of cyberattacks, according to a 2023 survey.

**51%** of organizations are planning to increase security investments as a result of a breach.3

**66%** of organizations are concerned about the extent of cyberattacks, according to a 2023 survey.

**51%** of organizations are planning to increase security investments as a result of a breach.3

**69%** of state officials are concerned about the extent of cyberattacks, according to a 2023 survey.

**51%** of organizations are planning to increase security investments as a result of a breach.3

**66%** of organizations are concerned about the extent of cyberattacks, according to a 2023 survey.

**51%** of organizations are planning to increase security investments as a result of a breach.3

**69%** of state officials are concerned about the extent of cyberattacks, according to a 2023 survey.

**51%** of organizations are planning to increase security investments as a result of a breach.3