protiviti®
Global Business Consulting

New White House Cybersecurity Strategy Creates Additional Concerns for Businesses

9 March
2023

The White House recently released a comprehensive national cybersecurity strategy that is sure to have a major impact on government agencies as well as private businesses.

The Biden-Harris Administration has been percolating a comprehensive cybersecurity strategy for some time and in early March released the aptly named "National Cybersecurity Strategy." The 35-page document was created to help strengthen cybersecurity on a national level and also address the lessons learned from the advanced cyberattacks that have taken place over the last few years. Many of those cyberattacks were designed to disrupt critical infrastructure, steal personal and/or proprietary (or classified) information, disrupt financial transactions and impede public services.

The administration's new cybersecurity strategy aims to address numerous weaknesses in cyber defences as well as change the perception of how the federal government reacts to cyberthreats. It also indicates that the U.S. government recognises that the technologies and processes in place have failed to keep the nation safe from cybercrime and potentially hostile nation-states, including but not limited to China and Russia.

The strategy sets forth a vision that redefines the nation's cybersecurity posture while also establishing new responsibilities for both businesses and government agencies. Although this vision has not yet become legislation, it will drive adoption of new cybersecurity processes, while also establishing the groundwork for creating new mandates that businesses and government agencies must adhere to.

The catalyst for change

Over the last few years, protecting networks in the U.S. from cyberattacks has become more complex and difficult. Incidents such as the ransomware attack on the Colonial Pipeline and the ransomware attack on JBS, the world's largest meat processing company, have demonstrated how vulnerable critical networks have become.

According to the Biden administration, both attacks originated from nation-state organisations. In both incidents, the White House offered help once notified of the attacks and involved the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI.

Those attacks (and many others) became the catalyst for further addressing critical infrastructure and changing how the federal government handled cybersecurity. In the past, orders and directives only applied to federal agencies and did not address private companies' critical infrastructure.

Recognising the shortcomings in current policies and directives, the Biden-Harris administration set out to reshape how the federal government could strengthen the nation's collective cybersecurity stance.

Five pillars of policy

Biden's cybersecurity strategy is broken down into five pillars, each of which has defined strategic objectives and, in ways both large and small, will likely affect private-sector organisations as well as government agencies and contractors. Those pillars include:

1. **Defend critical infrastructure.**
2. **Disrupt and dismantle threat actors.**
3. **Shape market forces to drive security and resilience.**
4. **Invest in a resilient future.**
5. **Forge international partnerships to pursue shared goals.**

Delving deeper into each of the pillars reveals some notable objectives and the potential for the federal government to work more closely with the private sector to improve cybersecurity hygiene. However, there are also some new responsibilities potentially being assigned to businesses which could have a profound impact on liability. In addition, the new strategy addresses the most active and persistent threats and proposes a more active role for the military, working with cloud services providers, to disrupt cybercriminal infrastructure.

Defend critical infrastructure

The first pillar of the White House's cybersecurity strategy notes the importance of protecting the nation's critical infrastructure and developing a collaborative model to defend important infrastructure assets. The strategy calls for a sharper focus on cybersecurity

regulations created to mitigate threats to U.S. critical infrastructure and recognises that a large majority of that infrastructure is owned and operated by the private sector.

From a policy perspective, this pillar will place a burden on private-sector businesses in the form of new regulations. Mandatory requirements will most likely be created that instruct the owners and operators of critical infrastructure to implement robust cybersecurity measures. However, the administration also seeks to level the playing field by ensuring that new requirements are operationally and commercially viable and tailored to each sector's risk profile.

The administration's strategy will encourage state and federal regulators to establish requirements that harmonise and streamline new regulations with existing cybersecurity regulations. State and federal regulators are also directed to collaborate in efforts to minimise harm where regulations are in conflict or are otherwise overly burdensome.

While the expected new regulations will create additional burdens for some business entities, there should be a significant payback in the form of better protecting infrastructure and the federal government being more prepared to help mitigate an attack.

Disrupt and dismantle threat actors

The second pillar is aimed squarely at the bad actors, be they individuals, criminal organisations or nation-states. Here, the federal government is seeking to enhance public-private collaboration to go on the attack and disrupt malicious actors. The strategy is based upon making integrated federal disruption activities more accessible to combat cybercriminals. The federal government also will seek to increase threat-intelligence gathering to identify emerging threats and criminal syndicates.

For many businesses, one of the objectives of this pillar may have a lasting impact on how an organisation deals with a ransomware attack. The federal government seeks to discourage paying ransoms while also disrupting illicit cryptocurrency exchanges. This may lead to legislation that makes it more difficult to pay ransom and encourages businesses to report the attack to the government.

Shape market forces to drive security and resilience

The third pillar ideates the reshaping of responsibility for entities that are in the best position to reduce risk and mitigate threats. Or put more simply, places the liability of cybersecurity with those who offer software and services. This shift in accountability for cybersecurity was driven by the recognition that organisations which eschew cybersecurity

best practices and only make a minimal investment in cybersecurity negatively impact the broader cybersecurity environment.

The strategy here is to hold the "stewards of data" responsible for the security of personal information that they control. Ultimately, that strategy will result in legislation to enforce responsibility and require that personal data is properly secured from unauthorised access.

Liability could also shift for businesses that build software and offer services if what is proposed becomes legislation. The strategy document indicates that regulators must reshape laws and regulations that govern liability for data loss and harm caused by cybersecurity errors, software vulnerabilities, and other risks created by software and digital technologies. The goal is to shift the liability from end users back to those entities that fail to take reasonable precautions to secure their software.

Key objectives include preventing software manufacturers and publishers from fully disclaiming liability by contract or other agreements. In addition, the administration recommends the development of frameworks to reduce the liability of companies that develop and maintain their software products securely.

Businesses that sell technology services and software to the federal government must also consider another element of Biden's plan. The nature of federal procurement of those products and services may change, whereby entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, misrepresenting their cybersecurity practices or protocols, or violating obligations to monitor and report cybersecurity incidents will be held liable. Such violations will be reported to the U.S. Department of Justice for potential legal actions.

Invest in a resilient future

The fourth pillar has numerous implications for how the nation will face the future and help to better secure critical infrastructure. One of the primary elements here is the development of a diverse and robust national cyber workforce. Today, there is a lack of sufficient cybersecurity professionals and an increased need for experienced talent.

Creating the training programs and resources to build a national cyber workforce could have a profound impact on businesses. Many organisations are constrained in their cybersecurity efforts simply because the resources are not available to harden network and mitigate cybersecurity issues. What's more, the White House's plan explains the need for deploying next-generation technologies, discovering and reducing systematic technical vulnerabilities and making the internet more resilient. With an eye towards future challenges, the White

House is also pushing for more research and development into cybersecurity technologies that will counter future threats, such as developing post-quantum encryption solutions and creating defences against attacks originating in the metaverse. Those objectives will need a workforce that is trained in technology and cybersecurity best practices.

Forge international partnerships to pursue shared goals

The fifth and final pillar recommends building international relationships that can increase collaboration and strengthen defences. Although these objectives are aimed at the governments of allied nations, there is a potential benefit for businesses that operate internationally. If the primary response of cybersecurity can be unified across nations, businesses that operate in those nations will be better protected and have local resources available to counter cyber threats.

On a global level, the U.S. is looking to leverage international coalitions and partnerships among like-minded nations to counter threats to the nation's digital ecosystem through joint preparedness, response and cost imposition.

Our Point of View

The Biden-Harris administration's cybersecurity strategy highlights the need for the government and businesses to work together to secure critical infrastructure, protect agencies and businesses from nation-state attacks, develop better defences, and take direct action against bad actors.

Although much of the strategy outlined can be considered basic best practices for cybersecurity, and ones that many or most organisations are undertaking today, the White House plan contains an element of vision and what the future holds for cyber in general. The federal government is taking cybersecurity and its impact on businesses very seriously and making disruption of businesses, supply chains, public services and utilities a matter of national defence. Organisations in or affiliated with these areas need to be fully aware of growing expectations among the federal government and other stakeholders.

Organisations can learn a great deal from the comprehensive policy the White House is offering, yet there is still a call to action to recognise. The winds of change are coming in the realm of cybersecurity, where attacks will become more complex and persistent, and defences will need to be improved.

Organisations can prepare themselves for the potentially radical changes envisioned by embracing these best practices:

- Create a comprehensive inventory of the organisation's infrastructure.
- Identify and document all security policies.
- Identify all critical assets and data (the organisation's "crown jewels").
- Determine what happens if these critical assets are lost or compromised – is the organisation positioned to recover them?
- Build a list of all software and services and determine responsibility.
- Identify all vendors and review licenses and contracts.
- Bring in professionals to test cybersecurity defences.
- Incorporate traffic monitoring and analysis.
- Take proactive steps to protect your enterprise from ransomware attacks.

Look for more information to come in the near future which will be distributed by the CISA.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, governance, risk and internal audit through its network of more than 85 offices in over 25 countries.

Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. Named to the 2022 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of *Fortune* 100 and nearly 80 percent of *Fortune* 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our Security and Privacy Practice

From the speed of innovation, digital transformation, and economic expectations to evolving cyber threats, the talent gap, and a dynamic regulatory landscape, technology leaders are expected to effectively respond to and manage these competing priorities.

To grow securely while reducing risk, your cybersecurity posture needs to adapt and respond to your business changing. As technology rapidly evolves and digital adoption accelerates, Protiviti's cybersecurity and privacy team turns risk into an advantage – protecting every layer of an organisation to unlock new opportunities, securely.

Our strategic and technical subject-matter experts fully understand your cybersecurity needs. We set out to assess, develop, implement, and manage end-to-end next-generation solutions tailored to your specific needs. We share your commitment to protecting your data and optimising your business and cyber resiliency.

protiviti®