SKYBOX SECURITY

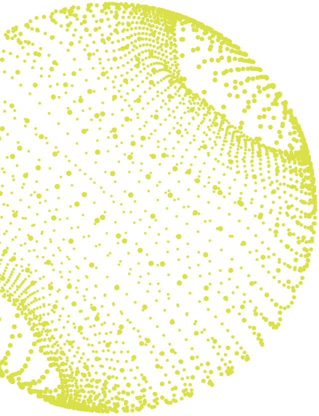
Biden's cybersecurity executive order calls for an expanded scope

A proactive and global security posture strategy is needed

At first blush, President Biden's executive order on national cybersecurity[1] may appear to be timely – a direct response to a series of crippling ransomware attacks on critical U.S. infrastructure. As the world attempted to recover from a devastating pandemic, hackers successfully targeted hospitals, then daily necessities such as food, water, and energy supplies, causing panic and disruptions. Immediate federal government action to address these and future threats is certainly necessary.

Unfortunately, the executive order is neither perfectly timed nor a comprehensive enough response to one of the most serious national security challenges of our time. The cybersecurity industry has been sounding the alarm bells on ransomware threats for years. Concerns were on the rise well before the pandemic, as organizations began accelerating latent digital transformations and expanding access to insecure operational technology (OT) assets. However, since the pandemic, this has been further compounded by the massive expansion of cloud migrations and meteoric rise in VPN deployments, opening up exponential numbers of new entry points for cyberattacks. There were consequences: Digitizing without adequate OT/IT security enabled hackers in Russia, North Korea, and Iran to seize control of key American businesses without even setting foot on U.S. soil – attacks that could have been prevented.

While the executive order is a "good first step,"[2] a "really ambitious plan…[that] should be effective if implemented properly,"[3] and an open acknowledgment[4] of the "outdated security models and unencrypted data [that] have led to compromises of systems in the public and private sectors," the U.S. federal government needs to adopt a new cybersecurity paradigm if it wants to stop today's threat actors. Crimefighting must increase its emphasis on nation-state cyber threats – given their increased prevalence sophistication – and shift from reactive to proactive.



A border-less world requires progressive thinking

This isn't the cybersecurity world of 10 years ago, where geographic borders and limited digitization served as walls keeping criminals from their targets. Today's businesses are borderless, as are their attackers. The latest threats have either geopolitical implications or origins; U.S. private sector organizations now face attacks encouraged or enabled by foreign governments. By the time threats emerge, their results are catastrophic, so everyone – the public and private sectors alike – needs to take a more proactive cybersecurity stance. It should come as no surprise, then, that the U.S. government's demand for vendor-based information security services and products is projected to increase at a 5.3% CAGR between 2019 and 2024, from $11.9 billion to $15.4 billion.[5] The volume, frequency, and sophistication of threats have become so serious that organizations are either protected, or they're prey.

[1] Executive Order on Improving the Nation's Cybersecurity, The White House, May 12, 2021
[2] Statement of Sen. Warner on President Biden's Cyber EO, The Office of Senator Mark R. Warner, May 12, 2021
[3] Krebs on Biden's Cybersecurity Executive Order: 'It's a Really Ambitious Plan,' The Hill, May 16, 2021
[4] Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks, The White House, May 12, 2021
[5] Government's Broader Role in Cyber, Deloitte, Amry Junaideen, et al., March 4, 2021

New trojans grew by **128%** in 2020

Precarious market factors necessitate a modern approach

The federal government struggles with many challenges as the private sector, including fragmented infrastructures, siloed functions, decentralized processes, resource constraints, and expertise gaps. A sophisticated threat landscape, increased complexity and speed, and significant resource drain have collectively kept top officials behind the curve of security incidents, enabling substantial breaches. In 2020 alone, malware samples almost doubled, ransomware increased by 106%, and new trojans grew by 128%.[6]

To address imminent cyberattacks, well-intentioned officials may have considered the executive order as the digital equivalent of directives that saw physical barriers go up at key federal buildings after the September 11 attacks – a measure that had to happen right away. Unlike physical walls, however, the process for simultaneously building cybersecurity perimeters around federal agencies and creating a centralized network to monitor them isn't as easy or fast. Any silver bullet offering that claims to fix everything is likely to be complex and expensive yet incapable of actually delivering on its bold promise.

Collaboration should be underpinned by a common view of data

Like the private sector, the public sector needs to create a mature, consistent, and enterprise-wide security posture management program. It also needs to create a standard view, processes, and communications to eliminate silos. The executive order does take steps in that direction.

For instance, Section 6 will help the federal government develop cross-agency standards[7] for responding to cybersecurity vulnerabilities and attacks to improve the cataloging of incidents and encourage progress towards successful responses. The order requires the Secretaries of Homeland Security and Defense to work with information councils and intelligence agencies to create a standard set of operating procedures for planning and conducting response activities, to be based on the National Institute of Standards and Technology (NIST) standards and used by federal civilian executive branch (FCEB) agencies.

This "playbook" will create a heightened minimum standard for responses and remediation while encouraging consistent use of key cybersecurity terms across both agencies and applicable statutes. That said, the playbook must be underpinned by cybersecurity technology that allows all parties to view the same dashboards and insights, so they can collectively make better, more informed decisions.

As David Wennergren, CEO of the American Council for Technology and Industry Advisory Council, rightly suggests, "collaborating with industry will be crucial to the success of this work… Changes in technology, to include moving to the cloud, IT modernization, operating in a virtual world, mobile solutions and the rapid adoption of new technologies all require that government collaborate with industry to understand best practices and new approaches, like zero trust."[8]

It's worth noting that the Cybersecurity Enhancement Act of 2014 updated NIST's role to include identifying and developing cybersecurity risk frameworks for voluntary use by critical infrastructure owners and operators. NIST is charged[9] with identifying a "prioritized, flexible, repeatable, performance-based, and cost-effective approach including information security measures and controls, that may be voluntarily adopted by owners and operations of critical infrastructure to help them identify, assess, and manage risk."

[6] Cybersecurity comes of age: Vulnerability and Threat Trends Report 2021, Skybox Security

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

[8] Who Will Pay for the Cyber EO Mandates?, GCN, Chris Riotta, May 23, 2021

[9] Cybersecurity Incentives: A Proposed rule by the Federal Regulatory Commission, Federal Register, The Daily Journal of the United States Government, February 5, 2021

Reported in 2020:

30,819

information security incidents across the federal government

Focus on risk exposure rather than deploying patchwork solutions

Like many large private enterprises, the U.S. government has an incredibly large attack surface: In 2020 alone, the White House reported 30,819 information security incidents across the federal government, an 8% increase from the prior year.[10] This playbook will only be helpful if federal government security and IT leaders can visualize and analyze their hybrid, OT, and multi-cloud networks to gain full context and understanding of the entire attack surface.

Section 7 of the executive order[11] focuses on securing federal government-owned networks using early detection of cybersecurity vulnerabilities and incidents, notably to increase overall visibility into individual agencies' network threats. The key provision of this section is a requirement that agencies deploy Homeland Security-approved endpoint detection and response (EDR) systems that will enable the federal government to actively hunt, contain, and remediate cybersecurity threats and respond to incidents without prior authorization from agencies.

While the order mandates agency adoption of endpoint detection and response systems, EDR is typical of prior-generation cybersecurity solutions: It focuses on what is currently happening rather than preventing exposures from spawning attacks.

Proactive prevention is the key to stopping intruders, and full lifecycle vulnerability management is a necessary component of that strategy. EDR alone cannot address either the process or resources needed to parse volumes of insights, nor can it identify where real-world exposure risk lies.

To fully identify and assess the exposure risk of vulnerabilities, security practitioners will need to see everything – from patch and EDR data to scanners, CMBD data, security controls, network configurations, and unscannable assets. Only after collecting and normalizing this data can the federal government effectively prioritize remediation efforts based on vulnerability exposure and exploitability.

Full lifecycle Vulnerability and Threat Management

Delivering pinpoint accuracy and efficiency over typical vulnerability management approaches

DISCOVERY

+ All scan data (multiple scanners)
+ Patch & EDR data
+ CMDB data
+ Security controls
+ Network configurations
+ Identified unknowns
+ Threat intelligence

PRIORITIZATION

+ Business impact
+ Exposure – viable attack paths
+ Exploitability
+ Severity by CVSS score
+ Efficacy - finding riskiest vulnerabilities
+ Age
+ Proximity - to most important assets

REMEDIATION

Planning:

+ Assess patch options
+ Assess non-patch options
+ Mitigation recommendations

Assignment:

+ Generate ticket
+ ITSM workflow
+ Provide context
+ Provide SLA
+ Communicate to ops teams

OVERSIGHT

+ Reconcile to SLA
+ Recalculate risk scores
+ Customer database enrichment
+ Reporting
+ CMDB enrichment

[10] Federal Cybersecurity: America's Data Still at Risk, Staff Report, Committee on Homeland Security and Governmental Affairs, August 2021

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

> Issues addressed in the Biden EO "will only be solved through years – **literally years of focus** and continued investment."
>
> - Matt Hartman, CISA Deputy Executive Assistant Director for Cybersecurity

An unrealistic timeline diminishes the order's impact

Unfortunately, some of the executive order's timelines are not realistic given the incredible complexity of the cybersecurity challenges the U.S. now faces. Most of the directives required long-ignored issues to be tackled within 30 to 60 days – time that elapsed before the real scope of the undertaking set in. But despite the severity of the threats, there aren't magical solutions that can fix everything within a month or two. As CISA Deputy Executive Assistant Director for Cybersecurity Matt Hartman points out, issues addressed in the Biden Administration's EO "will only be solved through years – literally years of focus and continued investment."[12]

This August, the industry will reassess the government cybersecurity landscape as we pass the 90-day mark of the executive order. Hartman adds that this milestone should be viewed as the first step in a long-term security journey, that "as we hit the end of the 90-day EO timeline, we will have many enduring plans with additional milestones that the White House, OMB, CISA and others will continue driving for the next several years, for the duration of this administration."[13]

This executive order was a call for security transformation. And transformation does not take 90 days. Organizations must shift deliberately – both culturally and behaviorally – from tools- and controls-based systems to a preventative, "modern digital infrastructure based on principles of zero trust"[14] that offers a long-term framework for a preventative cybersecurity posture.

Order punts the ball for the private sector

At this stage, the executive order is best understood as a collection of marching orders for federal agencies, accompanied by a suggestion that the private sector tries its best to keep up through a range of "mostly… voluntary measures for companies to meet a series of online security standards."[15] Rather than waiting to see how much the federal government achieves in the coming months, private organizations must begin or accelerate the process of securing themselves against cyberattacks, particularly since threat actors are likely to be inspired to act within the narrowing window of opportunity ahead of enhanced security.

It's time to supercharge intelligence sharing

While the executive order rightly focuses on enhancing cybersecurity information sharing between the private sector and federal government, improving the flow of information must be a much larger mandate for the private sector. Organizations must internally share and use information across groups to fuel proactive, informed decisions about their security strategies. Externally, there must be more global private sector intelligence sharing regarding attacks – an aim of the non-profit Cyber Threat Alliance, which is already backed by dozens of computing, networking, and security companies.

[12-13] CISA Sees Zero Trust Adoption Coming into Focus Under Cyber Executive Order, Federal News Network, Jory Heckman, July 5, 2021

[14] Why Data-Driven Cybersecurity Is Critical Now, Booz Allen Hamilton, May 23, 2021

[15] Biden Signs an Executive Order Aimed at Protecting Critical American Infrastructure from Cyberattacks, New York Times, David Sanger, July 28, 2021

Appropriate incentives are necessary

Perhaps the most significant omission in the executive order is its lack of measures to engage the private sector, which an accompanying White House Fact Sheet[16] identifies as the owner and operator of "much of our domestic critical infrastructure." The administration suggests that the private sector "follow the federal government's lead and take ambitious measures to augment and align cybersecurity investments to minimize future incidents." Rather than providing either funding or incentives to spur these investments, the order mandates IT-related information sharing between the private and public sectors, tightened security standards for "critical software," and consideration of federal labeling requirements for secure consumer software and IoT devices. The only private sector incentives contemplated by the order are designed to get manufacturers and developers to participate in those software and IoT labeling programs. This modest level of financial support is entirely inadequate, given both the criticality of private sector infrastructure and the scope of the security challenges ahead.

The federal government should approach cybersecurity with a similar approach to its handling of climate change, which is combining new emission standards with tax breaks and other incentives to make rapid, substantial progress. Some emerging cybersecurity initiatives are taking this approach, including a proposal that the Federal Energy Regulatory Commission "establish rules for incentive-based rate treatments for voluntary cybersecurity investments by a public utility," providing "cybersecurity incentives to public utilities that go above and beyond requirements of the CIP Reliability Standards and materially enhance the cybersecurity posture of the Bulk-Power System by enhancing the applicants cybersecurity posture substantially above levels required by CIP Reliability Standards."[17]

[16] Fact Sheet: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks, The White House, May 12, 2021

[17] Cybersecurity Incentives: A Proposed rule by the Federal Regulatory Commission, Federal Register, The Daily Journal of the United States Government, February 5, 2021

Three ways to advance security posture strategy

In place of federal government mandates, the private sector should forge ahead with its security transformation. Three areas that will significantly advance those efforts include:

1

Focus on exposure risk

Proactive cybersecurity starts with two things: a complete understanding of what needs to be protected and the ongoing intelligence necessary to pre-empt likely attacks. Once an organization can visualize its entire attack surface, including the exposure points, it can implement optimal remediation strategies.

However, the massive, ongoing barrage of new vulnerabilities makes prioritization challenging and floods security teams with limited resources. Over 60% of security professionals estimate that their organizations spend more than three hours per day validating false positives.[18] Rather than wasting valuable resources chasing huge volumes of vulnerabilities, organizations need to zero in on which vulnerabilities are exposed to threat actors and can cause real risks to network assets.

2

Introduce automation as table stakes

Rather than simply increasing human resources or tools to equally deal with every new threat, organizations need to move beyond the volume play and make cybersecurity investments that can efficiently tackle multiple issues.

In a recent survey of cybersecurity professionals, 95% of respondents indicated that the cybersecurity skills shortage and its associated impacts have not improved over the past few years; 44% said it has gotten worse.[19] Specifically within the U.S. government, a recent Senate report revisiting a 2019 study of agencies' cybersecurity preparedness found that seven of eight examined agencies still have not met basic cybersecurity standards and are operating unsupported legacy systems in 2021.[20]

It's a simple fact that network complexities and the scope of attack surfaces will only continue to grow, spawning an abundance of security process gaps that are easy to address solely through automation. "Data is the fuel that lets the defenders move faster than the attackers," explained Booz Allen Hamilton executive vice president Patrick Gorman, noting that "the future of cybersecurity is data-driven."[21] Implementing automation will be necessary to keep security teams ahead of threat actors, reducing their need to manually chase down every vulnerability as data grows exponentially in volume.

3

Shore up the supply chain

Organizations should also take the time to educate themselves on zero trust. The federal government is putting all its eggs in that basket, and the recent executive order "makes the zero trust imperative clear."[22] Still, the reality is that every organization needs to address zero trust in its own way. This isn't a one-size-fits-all cybersecurity solution; each network environment is different.

One clear area of potential zero trust concern is the supply chain – a necessary part of many industries and a massive point of potential weakness. Many of the past year's most significant public and private sector cybersecurity breaches have resulted from vulnerabilities introduced through their supply chains. And these chains are trending towards more complex and global, expanding access well beyond the organization. Consequently, organizations need to re-examine their business models with eyes towards their supply chains' impacts on their cybersecurity strategies, including potential vulnerabilities.

In its recent rule proposal, the Federal Energy Regulatory Commission addresses the supply chain risk head-on: "The global supply chain creates opportunities for adversaries to directly or indirectly affect the management or operation of companies with potential risks to end users that could introduce unintended threats to the system and necessitate rapid mitigating actions. It is important that public utilities make cybersecurity investments quickly to address these cybersecurity challenges as well as other emerging threats."[23]

[18] Edgescan 2020 Vulnerability Statistics Report

[19] The Life and Times of Cybersecurity Professionals 2021, ISSA and ESG, July 28, 2001

[20] Federal Cybersecurity: America's Data Still at Risk, Staff Report, Committee on Homeland Security and Governmental Affairs, August 2021

[21-22] Biden's Cybersecurity Executive Order: Five Transformations, The Hill, Patrick Gorman, May 29, 2021

[23] Cybersecurity Incentives: A Proposed rule by the Federal Regulatory Commission, Federal Register, The Daily Journal of the United States Government, February 5, 2021

The first step toward a new future

We're just several months past the Biden Administration's Executive Order, and the future impacts and adoption of suggested measures are not yet clear. Nevertheless, the order signals a bold and critical first step in a long-term journey to improve the cybersecurity posture of both the United States and its industries. As one senior administration official put it, the executive order "makes a down payment towards modernizing our cyber defenses and safeguarding many of the services on which we rely…It reflects a fundamental shift in our mindset – from incident response to prevention, from talking about security to doing security."[24]

The high-profile incidents of the past several months have belatedly crystallized cybersecurity's central role in U.S. national security and economic prosperity. President Biden's administration has taken a significant step in the right direction, but plenty of work still remains. From private sector incentives, to a holistic focus on risk exposure, to automated solutions and beyond, the public and private sectors must advance together following the executive order, then continue marching in tandem to ensure a robust and cohesive approach to cybersecurity preparedness.

Manage cyber exposure at scale

At Skybox Security, we believe that context and intelligence is crucial to fortifying our nation's cybersecurity programs. Skybox works with public and private sector organizations alike to develop stronger security efficacy through creating mature, consistent security posture management programs. Skybox is the only platform that gives teams with the ability to collectively visualize and analyze hybrid, multi-cloud and OT networks, providing a full picture of their attack surface.

This allows public and private sector organizations to get ahead of the security incident by looking for vulnerabilities in the same way attackers do. They can zero in on the vulnerabilities with the highest risk score, walk the path of a potential breach and understand if vulnerabilities are exploitable and exposed - all while determining the optimal remediation strategy.

Contact a Skybox Security expert to learn more about how our vulnerability and threat management and security policy management solutions can help you manage your cyber exposure at scale.

[24] Biden Orders Fed Cybersecurity Boost; Targets Prevention, Reporting, Breaking Defense, Brad D. Williams, May 12, 2021

ABOUT SKYBOX SECURITY

Over 500 of the largest and most security-conscious enterprises in the world rely on Skybox for the insights and assurance required to stay ahead of their dynamically changing attack surface. Our Security Posture Management Platform delivers complete visibility, analytics and automation to quickly map, prioritize and remediate vulnerabilities across your organization.

skyboxsecurity.com