MeriTalk
Improving the Outcomes of Government IT

JUNIPER NETWORKS | Driven by Experience™

Colonial Pipeline Hack Rockets Ransomware to Top of U.S. Security Agenda

Ransomware has rocketed to the top of the Biden administration's agenda as cyberattacks launched from the soil of U.S. adversaries have started to bite into key critical infrastructure.

The administration is bringing the full weight of U.S. policy to bear on the larger problem of cybersecurity and, in particular, the scourge of ransomware, which preys largely on less-sophisticated businesses that also happen to keep the country running.

The White House is also applying pressure on nation-state adversaries, rallying overseas allies, and issuing marching orders for the Federal government's cybersecurity apparatus to rethink and rebuild for better security and greater deterrence.

On Capitol Hill, lawmakers are cranking up similar efforts. Legislation in the works would back up the Biden administration's strategy and draw business into a more collective defense structure.

Further, the days of sitting on the sidelines are over for the private sector – especially American businesses considered critical infrastructure. Legal obligations – at the very least to disclose attacks to Federal authorities – look to be on the way.

Takeaway Number One – Unprecedented National Focus

The Federal push for better security is unprecedented and shows that cybersecurity is completing the leap from a technical problem to a national priority.

Tech dependence and attack sophistication have grown leaps and bounds over the past decade, and the fabric of everyday society is stitched ever more tightly with digital thread. When a ransomware attack on a pipeline company most people had never heard of turns into gas lines up and down the East Coast, that means the formerly esoteric issue of ransomware has become painful for everyone – and that pushes the odds higher for achieving lasting changes on the security front.

Takeaway Number Two – White House Elevates Response

The Biden White House is taking the most visibly assertive stance to improve cybersecurity – and deter ransomware attacks specifically – of any presidential administration in history.

Driving the urgency is a series of rapid-fire attacks that began before the administration took office and continued to spread through its early days – SolarWinds, Microsoft Exchange, Pulse Secure, Colonial Pipeline, JBS Foods. Suspicion that these attacks originated on foreign soil adds significant fuel to the fire for action.

Here are a couple of the administration's key steps and where they might lead.

First, the Cybersecurity Executive Order jolts the Federal government to overhaul security by migrating to zero trust security concepts and mandates endpoint detection and response capabilities that will allow the Cybersecurity and Infrastructure Security Administration to threat hunt across the entire civilian government enterprise. The order also puts the private sector on notice that the government will only be buying software that meets new security standards.

The order encourages private sector companies to follow the government's lead. It also paves the way for a tighter partnership down the road, saying that "cybersecurity requires more than government action."

Notably, the White House called the order "the first of many ambitious steps" it plans to modernize national cyber defenses, and specifically called out the SolarWinds, Microsoft Exchange, and Colonial Pipeline incidents as proof that cyber assaults from nation-states and criminals demand better defense.

In June, President Biden took the message overseas. He aimed to rally U.S. G-7 and NATO allies for cooperation on security standards-setting and closer cooperation on joint cyber defense efforts. He also confronted Russian President Vladimir Putin publicly for alleged complicity with attacks emanating from Russia-based actors.

The optics and the headlines from the June 16 Biden-Putin summit could not have been clearer – cybersecurity has risen to the top of the U.S. foreign policy agenda, and Biden's line in the sand is that critical infrastructure must be off-limits to attacks.

Takeaway Number Three – Congress Preps Legislation

Upwards of 80 percent of critical infrastructure is privately owned. Outside of highly regulated sectors, such as the power grid, Congress has been reluctant to impose binding requirements to achieve specific levels of security or support collective government cyber efforts.

Instead, many critical infrastructure companies have tied into private-sector threat sharing and analysis centers and may (or may not) opt to build security according to the voluntary standards provided by the National Institute of Standards and Technology (NIST). But at the end of the day, those largely remain smart choices to make, rather than requirements imposed by law.

The big-name cyberattacks since late last year primed the congressional pump on security issues. But it was the Colonial Pipeline attack in May and the JBS Foods attack in early June that changed the equation. The former attacks could be considered "tech" issues, while the more recent incidents translate into questions about basic consumer goods like gasoline and food and possible disruptions to critical supply chains.

Congress is responding along several lines of effort.

House Oversight and Reform Committee Chairwoman Carolyn Maloney, D-N.Y., has been pressing the corporate victims of ransomware attacks – including Colonial Pipeline and JBS Foods – for ransom payment information. According to reports, each company paid off its attackers, and the Justice Department acted to capture back a portion of the cryptocurrency payment made by Colonial Pipeline. Expect more from the committee to bring the details of attacks – usually kept secret by victims for fear of reputational damage – into the light.

Sen. Mark Warner, D-Va., predicted that legislation will soon emerge to mandate that private sector organizations report cyber incidents to Federal authorities. He expects the bill to have strong bipartisan backing and support from the Biden administration. The bill's aim, he said, will be to improve the government's awareness of cyberattacks that rely on ransomware demands and the ability of the Feds to take action against perpetrators. He also favors debate on whether payments to attackers should remain legal.

The senator also supports the creation of international standards around ransomware and the use by the United States of cyber offensive capabilities when possible.

Finally, Sens. Gary Peters, D-Mich., and Rob Portman, R-Ohio, who lead the Senate Homeland Security and Governmental Affairs Committee, are reaching out to the White House for President Biden's input on a ransomware bill they are drafting together. Part of their inquiry is for information about current strategies the government uses to combat ransomware and whether any legal authorities need to be updated. They are aiming to get a bill passed by August.

Notably, the two senators have already shown their ability to thread the 50-50 needle in the Senate by getting cyber response funding and incident reporting legislation wrapped into the U.S. Innovation and Competition Act (USICA) that passed the Senate in June by a wide margin.

Cyber Experts Weigh in – Policy

Officials from leading cybersecurity providers agreed that while Federal policy and legislative efforts to improve security and curb ransomware are pointed in the right direction, making a dent in ransomware ultimately will require targeted organizations to commit to technology improvements that make them less vulnerable.

> "The administration must consider the vital role that automation can play in preventing these attacks. Comprehensive, end-to-end security across IT is a must going forward.... As more operational technology devices come online and integrate with IT networks, the risk of cyberattack grows."
>
> ***– Bob Tafoya, Global Practice Lead – Critical Infrastructure and Industrial IOT, Juniper Networks***

Bob Tafoya, Global Practice Lead – Critical Infrastructure and Industrial IOT Juniper Networks, noted the immediacy of the Cybersecurity Executive Order's 100-day initiative to study ways to prevent attacks on energy delivery systems. "The administration must consider the vital role that automation can play in preventing these attacks," he said. "Comprehensive, end-to-end security across IT is a must going forward."

"I'm hoping the Colonial Pipeline attack is remembered not just for the 1970s oil crisis flashbacks, but as a catalyst for much-needed improvement in protecting our critical infrastructure," Tafoya said.

"The government mandate for a zero-trust security architecture is the first step of many to address ransomware," said Darren Guccione, CEO at Keeper Security.

"Cybersecurity policies need to specifically address password security and encryption because it is integral to establishing a comprehensive cybersecurity strategy," he explained. "Breach after breach, compromised passwords are often the root cause of the attack – over 80 percent of data breaches are due to weak password security and related control deficiencies. Cybersecurity password solutions must provide IT and security administrators with the ability to enforce password security best practices with visibility into adoption."

"The elevation of cybersecurity to the top levels of government policy," Guccione said, "is transformative – it allows government agencies to proactively address the threat landscape with essential cybersecurity tools like an Enterprise Password Management platform. This is critical to shift human behaviors that have historically increased cyber risk."

Mark Bowling, Vice President of Security Response Services at ExtraHop, charted the growth in ransomware attack sophistication over the past five years – from the days when many malware-based attacks compromised single servers or workstations – through the wave of WannaCry and NotPetya attacks that self-propagated through networks "to achieve massive reach and inflict maximum damage."

Important to current-day U.S. policy moves, he said those attacks "were the first well-documented examples

of prominent national-level criminal enterprises using ransomware as a cyber weapon to attack entire organizations," that set "a new standard for what ransomware could achieve."

Subsequent waves of attacks, including the Colonial Pipeline assault, have "brought into sharp relief how sophisticated these criminal enterprises have become," Bowling said. "In a sense, these attacks should no longer be called 'ransomware.' Rather, they should now be called the Advanced Extortionate Persistent Threat, maybe even EPT for short."

Bowling said he was less than hopeful that the current lineup of U.S. government responses will do much to turn back the attack trend, at least until those are accompanied by effective deterrence against nation-state intelligence agency APT attacks and EPT attacks from criminal enterprises. "We must, as a nation, resolve to take a harder, more aggressive, more punitive, and more penetrating response strategy – one that the Federal government and its intelligence agencies must lead."

He also advised the government to create safe-harbor rules for the private sector to report attacks, remove the anonymity and lack of regulation on cryptocurrencies, and provide financial incentives for organizations to improve security.

Curtin Simpson, Chief Information Security Officer at Armis, also tracked the historical path of ransomware attacks and why they have changed from the early days when encryption assaults could be overcome by having backup data.

"Today's ransomware attacks are commonly focused on critical infrastructure and operations that are inherently reliant upon operational technology (OT) and industrial control systems (ICS) technologies. Why? When an attack impacts or threatens to impact OT technologies, there is no ability to recover from a backup," he said. "Recovery involves ripping and replacing impacted devices, and depending on the level of compromise, such an attack can result in days to weeks of downtime."

"Very few operations can afford days to weeks of downtime, let alone critical infrastructure," he said. "If the bad actor is successful in their efforts to compromise OT/ICS, a payout is almost guaranteed. It is for this reason that OT/ICS environments are directly under attack on a daily basis."

"With eight-figure ransom payments becoming a more common occurrence, this will not slow down until controls are once again effective at preventing the attacks and the need for payment," Simpson predicted.

He credited the Biden administration's Cybersecurity Executive Order with establishing specific control requirements for software and services that the government will purchase. "Much of limiting the potential for ransomware-based attacks to materially impact critical infrastructure lies in the consistent implementation of effective core technical and procedural controls ranging from account protection to continuous monitoring," he said.

Simpson also explained that the White House order makes it "clear that future ransomware attacks with a material impact will trigger periodic reassessments and potential updates to the mandated controls and outcomes. This closed-loop review and update process will help ensure that mandated controls evolve with ransomware tactics and that we are not securing for only today but for tomorrow and beyond."

Bryan Rosensteel, Federal Solutions Architect at Ping Identity, explained that while the Colonial Pipeline attack made big headlines, the "incident was not the

first ransomware attack that resulted in a loss of services. Several major U.S. cities have had their systems infiltrated and data seized, impacting first responder systems and other critical infrastructure components."

"These components are very compelling targets for ransomware attackers, as the greater the public impact, the higher the ransom they are likely to receive," he said.

On the policy front, he said, "it will be interesting to watch how cyber relations between the U.S. and Russia develop on the heels of the Biden-Putin summit."

"It is clear that there is pressure for the Biden administration to hold nation states accountable for the cyber activities that occur within its border; however, we have yet to see whether the administration will take a more collaborative or combative approach to do so," he said.

Cyber Experts Weigh in – Technology

We also asked the experts what initial steps companies can take to avoid becoming ransomware victims and found that many of them involve better cyber hygiene through the use of automation technologies.

"Ransomware is the term that usually makes it into the headlines; however, social engineering, email phishing, and malicious links – including QR codes – are some of the major vectors used to deploy ransomware," explained Bill Harrod, Vice President of Public Sector at Ivanti, who also pointed to recent studies showing that many successful attacks begin with compromising mobile devices.

Harrod stressed the importance of "establishing a contextual relationship between the user, their authorization (credential), the network, policy compliance, and the target application or data that they are accessing."

Further, Harrod said, "Unpatched vulnerabilities and default configurations are another common point of entry into public sector organizations' ecosystems. Public and private sector companies frequently are behind in their patch management process, due in part to the lack of resources needed to patch every vulnerability manually."

"Hyper-automation technologies that are powered by deep intelligence and use supervised and unsupervised machine learning algorithms can drastically improve IT defenses," he counseled. "They provide organizations

with visibility over all endpoints, applications, and data, and can effectively manage their security and self-healing capabilities with minimal human intervention."

Ping Identity's Rosensteel pointed to taking better care of identity and access management issues and not leaving easy avenues open to attackers.

"Many ransomware attacks do not involve overly complex exploits. It usually comes down to a compromised and/or often overused password coupled with a lack of multifactor authentication (MFA), or a weakness in a perimeter defense, such as a firewall or VPN," he said. "Once inside, there are usually very few additional barriers to prevent the attack from continuing."

"In the case of the Colonial Pipeline attack, a single password compromise on a legacy VPN that did not have MFA in place allowed the attackers to infiltrate the network and conduct the attack," Rosensteel said. "These weaknesses are perfect for the ransomware industry because they require little effort to execute and often are associated with other poor practices such as a lack of data backup that make the chance of payout higher – and getting paid is what these attackers are after."

"We do see some targeted attacks that are politically motivated, but the majority are simply to turn a profit," he said. "That's why most attacks revolve around relatively simple exploits and vulnerabilities."

Juniper's Tafoya said that energy and utility companies must first understand the unique threat landscape they face, including reliance on internet-connected devices and the need to increasingly rely on intelligent technologies.

"These organizations are increasingly relying on internet-connected industrial control systems to handle the various operational aspects of managing and monitoring fuel transmission and distribution," he said. "As more operational technology (OT) devices come online and integrate with IT networks, the risk of cyberattack grows."

"Private sector companies in critical infrastructure also must rely on intelligent technology – artificial intelligence (AI), machine learning (ML), and related technologies – on the OT side to automate repeatable tasks," Tafoya said. "Relying on machines rather than people is not only faster and cheaper, but it eliminates the chance of introducing human error that can lead to security flaws."

ExtraHop's Bowling shared a list of steps that critical infrastructure companies need to take to decrease their exposure, starting with developing a risk management strategy and getting executive stakeholder support. Then, he said, companies should develop their most appropriate technical cybersecurity framework, "irrespective of your regulatory compliance framework – regulatory compliance is not equal to effective cybersecurity."

"Then build your cybersecurity program around the technical framework that is best for you; probably either NIST CSF, ISO 27001, COBIT, or NIST 800 53R5," he advised.

Armis' Simpson argued that visibility is paramount for critical infrastructure providers. "First and foremost, operations that are critically reliant upon OT/ICS technology should invest in the capability to discover and identify all networked IT, IoT, and OT devices within their facilities."

He said the next step is to "apply a cyber resilience lens against the OT/ICS environment" to identify critical services and their underlying support technologies, and then assess those for high-risk exposures and develop mitigation and remediation plans. "Patching will be critical for backplane devices like network infrastructure but will often not be an option for existing OT and IoT assets," he said. "Rather, focus on restricting and constraining communications wherever possible."

"Ransomware attacks are now seen as a 'when' rather than an 'if' scenario," said Keeper Security's Guccione. "Companies need to mandate the use of a password management platform to properly secure critical functionality and security gaps left after single sign-on or privileged access management implementations."

"Password security is a human-centric approach to cybersecurity that often becomes neglected and leads us to the ransomware crisis that currently plagues the private and public sector alike," he said. "Administrators are able to enforce adoption of proven cybersecurity practices like MFA and seamlessly roll out the solution to employees all while maintaining zero-trust and zero-knowledge."

Finally

Difficult things are never easy to get done, and even more so with very slim margins in Congress and lingering national political divisions.

But what sets apart the issues of cybersecurity and ransomware are growing public awareness and concern that demands a government response and a startling degree of bipartisanship on the primary aims of improving security. There is plenty of room to debate the details of how to get there, but few seem to doubt the value of the destination.

With the Biden administration well on its way through domestic and overseas policy measures and Congress not too far behind, a shift in the playing field – and better security eventually – look to be a strong bet.