Ransomware attacks are increasingly prevalent and common among state and local governments, posing an urgent threat to infrastructure entities and national security. The Cybersecurity and Infrastructure Security Agency has posted best practices and related guidance to help stop ransomware attacks, and agencies are partnering with industry to share information and combat the threat together.

Four security experts from the government, industry and not-for-profit sectors gathered at a recent FedInsider webinar to discuss their shared efforts and the necessary steps they’re taking to secure the nation from ransomware.

The following are some of the most important aspects of those efforts.

The Increasing Risk of Ransomware

According to Mike Moran, special agent for the U.S. Secret Service’s Criminal Investigative Division, ransomware threats to the government are bad, and getting worse. “The threat actors right now are winning because they’re operating from countries that provide no assistance to U.S. law enforcement. And with these payments that are going out, the numbers are just astronomical with what these ransomware dollar values have gotten to,” Moran said.

Untaxed profit margins and the low-cost need of a few coders to exploit a system are driving bad actors. In other words, Moran said it’s a good time to be a criminal. “We are trying to make their life as difficult as possible, but until we have multinational support and actual penalties for assisting and aiding and abetting these criminals, then we’re going to kind of be at a loss,” he said.

Valecia Stocchetti, senior cybersecurity engineer at the Center for Internet Security, Inc (CIS), agreed with Moran’s sentiments. As long as the criminals behind ransomware attacks get paid, they’ll continue. “Ransomware is this nagging thing that just won’t go away,” Stocchetti said. “It’s for all organizations.”

Bad actors organize together to pull millions of dollars from impacted businesses and organizations, and attack surfaces are only expanding with the increased reliance on technology.

“It’s difficult it is to defend against and easy it is to attack. When you combine that with a profit and target rich environment, we can expect the threat landscape for ransomware to continue to grow,” added Ben de Bont, Chief Information Security Officer of ServiceNow. Despite the risk, this is also an area of opportunity, de Bont said.

Plan a Coordinated Response to Ransomware Attacks

When an organization is hit by a ransomware attack, de Bont said the first thing to do is to respond – even if there doesn’t seem to be a clear path forward yet. "It’s often better to make any decision than to correct moving forward as you narrow in on that incident’s situation," de Bont said.

Coming Together to Combat Ransomware

In an ever-evolving threat environment, the private and public sector must work together and share resources to protect the nation from ransomware attacks.
Siloed organizations, however, may slow down response capabilities. Stocchetti said siloes can even hinder recovery efforts, especially when personnel can’t take a system offline because a higher-up won’t let them. “When there’s that breakdown in communication and coordination, that’s something that goes south,” Stocchetti said. In fact, organizations can get hit a second time after the first attack due to the poor execution of their recovery efforts.

“There’s an importance of having a plan, and that you are executing it appropriately and methodically,” Stocchetti said. “You don’t plan for fire safety when there’s a fire in the building. Same thing with cyber.”

Experts recommend that investment, time and focus needs to be spent on people, process and technology to prepare for an incident like ransomware. That preparedness must also cross those siloes. This is because cyber incident response may require non-incident response personnel – like developers, legal support, law enforcement and so on. If the organizational business strategy needs siloes, create cross-functional execution across those siloes.

Plan for When – Not If – Your System Is Attacked

Along with ensuring a response plan is in place, Stocchetti recommends CIOs and CISOs securely configure systems, especially externally facing systems or business critical systems. After establishing baseline configurations, make sure to do change management and audits of those settings since configuration settings can change over time as software gets updated.

Echoing the importance of preparedness, de Bont noted that ServiceNow’s approach considers both potential and likely exploitation paths and preemptive testing against common attack vectors. “For technical testing, we’re looking at how vulnerable some of it might be,” de Bont added.

ServiceNow tests and monitors ransomware samples against its endpoint protection. It also does external password guessing and automated breach and attack simulations to provide improvement suggestions on the effectiveness of technology stacks.

For control testing, de Bont said the company focuses on how prepared it is for the future, and determines controls that are relevant to preventing and recovering from attacks. To do this, it partners internally with audit and enterprise risk teams. The outcome is quantitative and qualitative data about areas that need improvement.

In terms of recent attacks on supply chain vendors, government agencies and the CISO community are working together to share intel, approaches, tools and technologies to strengthen the IT supply chain.

Leveraging the Right Tools to Combat Ransomware

There is potential in using advanced technologies like automation, artificial intelligence and machine learning to help respond to ransomware. These tools can assist with behavior-based defense, so that IT teams can better understand the actions the attacks take, like the calls they make to other documents and areas of the network like endpoint devices. “Those are going to be your best line of defense,” Moran said.

For organizations with security operation centers, automation and machine learning technology can help operators do their jobs more efficiently. “If they’re responding to your typical flood of false positives or false negatives or doing mundane repetitive tasks on a day-to-day basis, then they’re going to be a lot less motivated to focus on looking at actual kill chains or working on other things they can be doing to improve your response capabilities,” de Bont said.

However, because government agencies don’t have private sector-type security budgets, Stocchetti stressed the importance of continuing to share low-cost services through the Information Sharing and Analysis Center and CISA. CIS provides the Malicious Domain Blocking and Reporting service, for instance, which is available to government members of the Multi-State Information Sharing and Analysis Center.

Finally, avoid paying ransoms, Moran said. Instead, put that money toward improving and investing in automated backup processes. “At the end of the day, you want your information back. Beef up the backup process and make sure that you have offline backups so they can’t also be locked down,” Moran added.