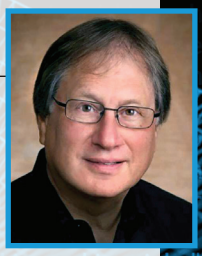
FEDInsider

Preventing and Recovering from the Increasing Number of Ransomware Attacks

State and local governments are addressing how to prepare personnel, technology, systems and networks for data breaches.

Featured Experts:

- **Alan Shark**
  V.P. Public Sector & Executive Director, CompTIA Public Technology Institute



- **Kevin Walsh**
  Director, IT & CS, Government Accountability Office

- **Peter Miller**
  Chief Security Officer, Orange County, Florida

- **Tony Lauro**
  Director of Security Strategies, Akamai Technologies

State and local agencies, health care systems and educational institutions have become heavy targets for ransomware attacks over the past few years – partly because they lack strong cybersecurity expertise and the resources to improve cybersecurity measures. Cyber liability insurance can help, but may require specific precautions to be put in place in order for an agency to qualify for it.

Experts agree, however, that good cyber strategies include risk assessment and mitigation. Government and industry leaders spoke at a recent FedInsider panel to discuss strengthening cybersecurity to prevent breaches, and the role cyber insurance can play in avoiding the impacts of ransomware. The following are some of the most important aspects of their discussion.

An Advanced Cyber World

The number of cyber incidents and the sophistication of cyberattacks have exponentially grown over the past several years, noted Kevin Walsh, director of IT and cybersecurity at the Government Accountability Office. He said this is most concerning to the agency. "It is scary how frequent and how bad some of these are getting," Walsh said, from both nation state and non-nation state actors.

Bad actors are also going for the data an organization values most – the data that is at highest risk if exposed, like health data. "The bad actors are looking to make a profit or to do damage," said Tony Lauro, director of technology security and strategy at Akamai.

Components of Proper Cyber Hygiene

Avoiding cyberattacks and mitigating cyber breaches requires a mix of people, software, hardware and governance. Part of that includes asset management and inventory, said Alan Shark, vice president of public sector and executive director of CompTIA Public Technology Institute.

"How do you manage what you don't know?" Shark asked. "What is it that you have? What is it you have to protect?" Conducting an inventory to know where IT resources are and who has access to them is critical. This works with personnel, too. Shark recommends surveying staff to understand how up to date they are in terms of their technical education and knowledge of the latest developments.

Then, dig into the quality of the technology and ask, are these the right tools for protecting against cyber intrusion? Have incoming traffic analyzed and then ask if it is as clean as it can be. Most digital intrusions happen because of human error – make sure the latest patch is installed.

"It is still important to make sure entire organizations see cybersecurity as an all-of-government type of affair. That includes cyber training," Shark said. Ensure personnel are aware of the latest cyberattack techniques and cybersecurity tools.

Lauro added that to limit the cost of a breach, organizations should reference the Cybersecurity and Infrastructure Security Agency and National Institute of Standards and Technology's cyber resource center and cybersecurity framework. "There are resources out there and people that want to help protect you," he said.

Ultimately, the first step to ensuring data accessibility during a breach or natural disaster is having an incident response plan. "That should walk me through everything," said Peter Miller, chief security officer of Orange County, Florida. "If I don't have that or if it is not detailed or kept up to date, that is when I start seeing problems. I would start there before I get into technology."

Understanding Cyber Insurance

Cyber insurance is meant to protect businesses from internet-based risks and limit the impact after an incident happens. It's not meant to be the first line of defense, as prevention and protection are key. Still, it's a must-have, but some products require certain cybersecurity protocols to already be in place before the insurance is applied. According to Lauro, those may include having a risk assessment done in the systems using the security controls, identifying where the vulnerabilities are and providing a plan for strengthening the security program.

These risk assessments may require the use of multifactor authentication for all employees, ensuring all systems are equipped with antivirus software and having a backup system in place. And as cybersecurity evolves and the stakes get higher, the cost of coverage will evolve, too.

It is also important to note that insurance coverage and providers will vary from organization to organization. Breach insurance, for instance, notifies those who are exposed as a result of a breach and can provide data restoration and credit monitoring. Cyber liability insurance is broader, and can include incident response, extortion costs, business interruption response and more.

Shark added that with these requirements, insurance companies are also making it more difficult for local governments to qualify. The application itself forces organizations to truly assess their cybersecurity posture and vulnerabilities, and to "develop strategies to address the weak links you have identified, knowing there will be some you cannot identify or do not know about," Shark said. "To qualify, it means you have to go through a lot of hoops which I think is good regardless. It should be the blueprint of where you start."

Getting on the Right Cyber Track

Considering a large number of incidents can be traced back to human error, organizations should first ensure their workforce is fully aware of cyber threats and the cyber landscape through an active program of information.

Shark suggested testing employees by sending a USB drive or an email with a link from a fake (but real looking) email address and seeing who opens them. If they do, they get flagged to IT. This can encourage a culture of awareness and ensures the system is being adequately monitored by an internal team or third-party provider. "Therefore, all incoming and outgoing data is being carefully examined looking for anomalies," Shark said. This is where artificial intelligence technology comes into play. There are tools that can scan and look for anomalies constantly, so personnel don't have to.

"Machines today can do things we could never dream of doing in fractions of a second. Maybe even a millisecond. These are the new tools that local governments and small entities need today to supplement the human value of making sure all our systems are brought up to date," Shark said.

Upskilling the workforce and investing in strong endpoint management to limit what goes in and out of the network remain top priorities, Miller said. And with the right governance in place, better state and local government communication and the anticipated federal funding for boosting local cyber hygiene, agency leaders can make better decisions about which tools and technologies are right for their organization. And that can keep agencies safe, even as the threat level continues to rise.

Hosky Communications Inc.
3811 Massachusetts Avenue, NW
Washington, DC 20016

(202) 237-0300
Info@FedInsider.com
FedInsider.com
Facebook.com/FedInsiderNews
Linkedin.com/company/FedInsider
@FedInsider

Carahsoft
11493 Sunset Hills Road, Suite 100
Reston, VA 20190

(703) 871-8548
Info@Carahsoft.com
Carahsoft.com/Akamai
Facebook.com/Carahsoft
Linkedin.com/company/Carahsoft
@Carahsoft

Akamai Technologies
11111 Sunset Hills Road, Suite 250
Reston, VA 20190

(617) 444-3000
Info@Akamai.com
Akamai.com
@AkamaiTechnologies
Linkedin.com/company/Akamai-Technologies
@Akamai