FEDInsider

Prepping & Preventing Damaging Cyber Attacks in Government

Devastation from cyberattacks can rival those of natural disasters, so government & industry are working together to prevent, respond & recover.

Featured Experts:

- **Bob Costello**
  Chief Information Officer, CISA

- **Paul Blahusch**
  Chief Information Security Officer, Department of Labor

- **Tim Goodwin**
  Chief Information Security Officer, U.S. Patent & Trademark Office

- **Travis Rosiek**
  Chief Technology Officer, Public Sector, Rubrik

The White House issued Presidential Policy Directive 40 in 2016, creating a national policy "to maintain a comprehensive and effective continuity capability by ensuring a coordinated effort within and among the executive, legislative and judicial branches of the government." This resilience has been critical during the war in Ukraine, considering the rise in cyberattacks and data breach attempts. All of that makes data protection more important than ever in government, with data management becoming a fundamental element to both the protection of information and remediation efforts following an attack. A successful data management approach yields other benefits as well, including regulatory compliance, cost reductions and enhanced system performance.

Thought leaders from government and industry spoke at a recent FedInsider webinar to discuss the importance of data backups and recovery in volatile cyberspace.

THE IMPACTS OF CYBERATTACKS

Dr. Gregg "Skip" Bailey, the Assistant Director for Cyberattacks, much like natural disasters, have the devastating potential to take down power grids, impact infrastructure, halt necessary transportation and healthcare services, disrupt financial systems and access to money or global markets, plus so much more.

"It is very difficult for individuals and communities to recover from cybersecurity attacks," said Tim Goodwin, chief information security officer of the U.S. Patent and Trademark Office. "We are naturally integrated with technology and infrastructure. It's almost impossible to understand the many dependencies we have just going through our daily lives."

Yet unlike some natural disasters where there is little to no advanced warning, cyberattacks can impact systems for months before IT teams realize an attack occurred. "The ongoing effects of the attack are difficult to understand," Goodwin said. "Who has my data? Where has my data gone? What are the impacts of the data, what data is vital to businesses or the economies around the U.S. or the world?"

Also, natural disasters are largely localized and response efforts are organized, but cyberattacks can be further-reaching depending on the system they disrupt. "In a cyberattack, or any sort of IT issue, it is how you plan and respond. And how well your teams are ready to do that," said Bob Costello, chief information officer for the Cybersecurity and Infrastructure Security Agency. "We need to build capacity in the cyber arena to respond the same way we have learned to respond to natural disasters...I think it is an area we all need to concentrate on, including the public and private sectors together."

Still, these impacts carry the same weight and criticality as those caused by natural disasters and can impact citizen trust in the nation's systems and services as the public depends on them.

ENSURING RESILIENCE

Federal systems and services can't risk catastrophic disruptions of normal operations. CISA's emergency communi-

cations division, for instance, oversees the continuity of government and ensures critical communications get through day-to-day and during times of communication network overuse. These telecommunications services are available to CISA's partner community, Costello said. CISA is also working with the industry to secure software design from the start and make multi-factor authentication the norm.

Resilience also depends on a security-first community alongside a shift in user mindset. Paul Blahusch, chief information security officer for the Department of Labor, said robust awareness programs for all employees are necessary to keep the department and its mission safe. "There's a great culture of preparedness and awareness amongst the user community," Blahusch said. They're focusing on engaging with a community to instill behaviors that would be beneficial to the department while identifying those that should be avoided. "We need to make it as easy as possible for people to do the right things with security, and hard to do the wrong things," Blahusch said.

Implementing a zero trust architecture also helps with data loss prevention and breach detection. It's about making it as difficult as possible for an adversary to get into the network in the first place.

"If an adversary does get to me, what zero trust does is really put a lot more information at the hands of my incident response team so they can detect it quickly, and shut it down before it causes a lot of damage," Blahusch said. And even if all else fails and an adversary does get in, micro segmentation means they can't compromise the wider network. "It can limit the exposure, which helps with your recovery effort."

PLANNING & PREPARING

The worst time to test processes and tools is during an actual crisis, said Travis Rosiek, chief technology officer for public sector at Rubrik. "The tech hasn't been updated and IT changes rapidly, so not exercising your processes, waiting for disaster to happen and then figuring it out on the fly is a recipe usually for disaster."

That's why it's critical to build resiliency from the beginning and ensure data backups. "Having these processes in place and being prepared and knowing who to contact, and streamlining all of that to make sure it's current," is critical to resiliency, Rosiek said.

"Specifically talking about backups, make sure you have a good recovery point to go back to in time," Rosiek added. "Because if you don't know how to determine a safe recovery point prior to an attack, then it's really going to make the problem worse and you will lose confidence and trust in your constituents and customers."

Federal services and response tactics via CISA, the Department of Homeland Security and FEMA are also excellent resources for planning and preparing for cyberattacks and disruptions caused by disasters, Costello said. Those agencies have decades of collective experience responding to emergencies and disasters, and it's imperative that the public and private sector work together to minimize the possible threats and aftermaths of cyberattacks.

And ultimately, Blahusch said prevention starts with patched systems, minimizing exposure, and training and awareness programs. "Your end-user is still one of the largest and most prevalent entry points for the bad guy," he said. "As security practitioners, we need to do a better job there of making sure that security is easy for these people. And still, we need to ensure we have got their awareness."

FEDInsider

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

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

rubrik | public sector

Rubrik
3495 Deer Creek Road
Palo Alto, CA 94304

(650) 300-5962
Rubrik.com/industries/federal-government
Facebook.com/RubrikInc
Linkedin.com/company/Rubrik
@RubrikInc