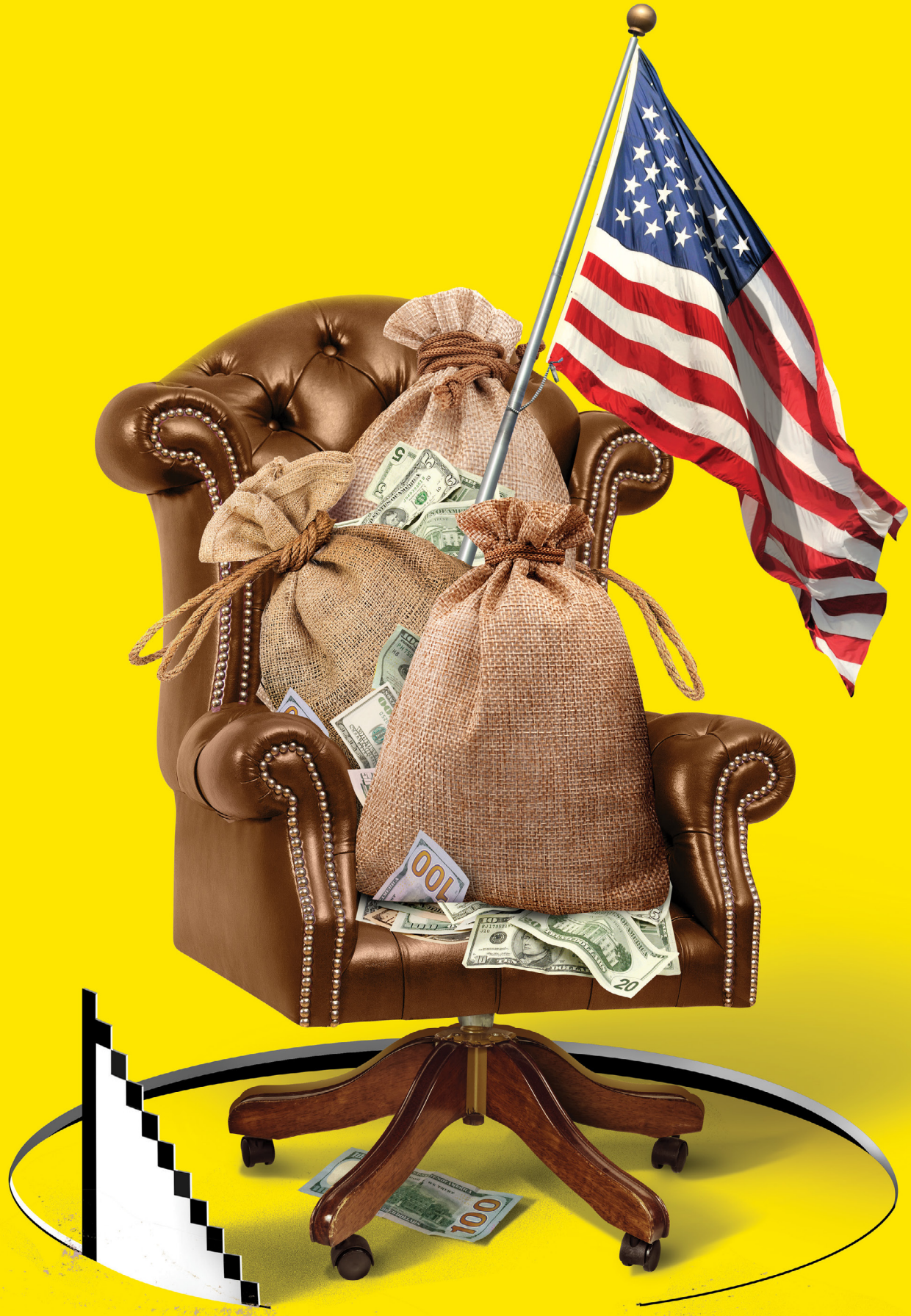

TARGETED FOR RANSOM

Government facilities rank third on the FBI's list of targets in ransomware schemes.

BY DAVID DIMOLFETTA

GOVERNMENT FACILITIES WERE the third-largest critical infrastructure sector targeted by ransomware attacks in 2023, according to cybercrime statistics released in March by the FBI.

The agency's Internet Crime Complaint Center, or IC3, unveiled the findings in its annual report that unpacks complaints, financial losses and other metrics used to determine the severity of cybercrime activities reported to federal authorities.

Of the 1,193 complaints IC3 received from organizations belonging to U.S.-designated critical infrastructure sectors, government facilities came in third place with 156 complaints, while critical manufacturing and health care centers took the second and top spots, respectively.

"Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 sectors had at least one member that fell to a ransomware attack in 2023," the report noted.

LockBit, ALPHV/BlackCat, Akira, Royal and Black Basta were the top ransomware gangs tied to those critical infrastructure complaints, the report added. ALPHV, which earlier this year claimed responsibility for its attack on Change Healthcare that caused widespread logjams in the prescription drug market, reportedly staged a takedown after hauling away a $22 million ransom payment from the company.

Ransomware operatives targeted companies around the world last year, with the number of firms targeted reaching an all-time high compared to findings in previous years, according to a January Check Point analysis.

The U.S. has been working with international partners to take a firm stance against ransom payments, though experts have not agreed on a single policy.

"The FBI does not encourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Paying the ransom also does not guarantee that an entity's files will be recovered," IC3 says.

IMPERSONATION SCAMS ON THE RISE

The IC3 report also found $350 million were lost from scams in which hackers impersonated government officials attempting to collect money. Older adults are overwhelmingly targeted in such scams, according to the data.

A total of 14,190 government impersonation scams were logged last year, up from 11,554 in 2022. The FBI previously said that some $55 million were lost to impersonation scams filed to IC3 between May and December last year.

DOUG CHAYKA

The Federal Trade Commission in February finalized a measure that would empower the agency to go after entities that impersonate government officials and others using AI tools. The commission took its first such action May 23, proposing a $6 million fine against the political consultant behind a robocalling operation that allegedly disseminated phone calls featuring an AI-generated voice of President Joe Biden ahead of the New Hampshire primary. //

RISK MANAGEMENT

NIST offers new security standards for sensitive info

BY DAVID DIMOLFETTA

THE FEDERAL ECOSYSTEM was supplied with a new set of security standards in April aimed at preventing the unauthorized transmission of sensitive unclassified information that's frequently exchanged between agencies and private-sector contractors.

The release from the National Institute of Standards and Technology updates the 2020 iteration of the document, adding three new families of security controls to the government's Controlled Unclassified Information program, which sets benchmarks for how federal agencies should safeguard sensitive unclassified data stored in their systems.

Chief among the new additions is a supply chain risk management framework that considers frequent collaboration between federal agencies and private-sector vendors that provide the government with software, equipment and training needed for everyday tasks. The other new families include an acquisition section for outside service providers, as well as an overarching supervision section to help agencies plan ahead for additional security controls.

Under the updated NIST standards, the U.S. government will have a year to transition existing operations to the new CUI caliber, while new federal programs will have to meet the threshold right out of the gate. Dozens of data types fall under CUI, including personal military records, export control research and internal intelligence community data.

The CUI label is applied to internal agency or Department of Defense information that is not deemed sensitive enough to be "classified" — so that only those with security clearances may access it — but that does pose risks if not protected.

SUPPLY CHAIN ATTACKS

Agencies and contractors often transfer data across devices or take their work home with them, and NIST believes a compromise of that data poses national security risks. CUI can range from personal health information in an agency's HR system to weapon systems documentation in the Pentagon, said Ron Ross, a co-author of the new framework who serves as a NIST fellow focusing on federal cybersecurity and risk management.

Supply chain cyberattacks involve a hacker using vulnerabilities in a third-party entity to breach the systems of another organization. In the case of the federal ecosystem, if U.S. data makes its way into an outside service or security provider, it may be vulnerable to hackers if not adequately protected.

"We're building a very complex infrastructure of information systems," Ross said in an interview with Nextgov/FCW. "You're talking about trillions of lines of code and billions of devices from industrial control systems to enterprise IT systems, devices ... firmware and software."

No single cyber incident motivated NIST to add a supply chain family to its new framework, but federal public-private partnerships mean "we have to ensure this information is protected," Ross said.

For example, supply chain cyberattacks last year involved a vulnerability in the MOVEit file transfer software that affected thousands of organizations around the world, as well as a separate incident where North Korea-linked hackers breached the 3CX conferencing app through a capital markets trading platform.

More recently, Microsoft came under fire for vulnerabilities that allowed Russian hackers to exfiltrate agency email exchanges with the company. The tech giant was also the subject of a scathing Department of Homeland Security oversight report following an attack last summer that allowed Chinese hackers to nab the emails of top U.S. officials, including Commerce Secretary Gina Raimondo.

"[CUI] has one common characteristic: The adversary knows this information has great value, especially things in research and development, which may take us years and years of very significant investment," Ross said. "And if adversaries can steal the information and turn it into the next-generation weapon system on their side, they don't have to invest all that money in their R&D." //

D3DAMON/GETTY IMAGES

TEN TIPS FOR PROTECTING YOUR AGENCY'S MISSION-CRITICAL DATA FROM CYBERATTACKS

GOVERNMENT AGENCIES ARE prime targets for cyberattacks, particularly ransomware. With ransomware, cybercriminals encrypt vital data to gain financial information, disrupt public services, threaten military operations and erode overall public trust in government. In a recent industry survey of 1,200 CISO, senior executive, cybersecurity and backup professionals, 76% of responding organizations recognize a 'protection gap' exists between how much data they could afford to lose and how their data is currently protected.[1] In fact, U.S. federal government survey respondents indicated a ransomware attack was more than twice as likely to affect all or most of their cloud-hosted data vs. on-premises data.

Salim Ruffin, senior engineering manager for Veeam Software, a global leader in data protection and ransomware recovery, discussed how to close this protection gap by starting with a disaster readiness assessment and continuing with implementation of regular updates to your hybrid cloud data protection strategy.

Here are some tips Ruffin shared.

1. **Educate and coordinate:** "Create a continuous learning culture of cyber awareness. Train employees and contractors and practice with simulated attack-response exercises on a regular basis," says Ruffin. Closer coordination between IT operations and cybersecurity teams can result in earlier threat detection due to enhanced situational awareness.
2. **Shared responsibility model:** While cloud service providers (CSPs) like Azure, AWS and GPC offer great service availability, it is your agency's responsibility to protect its cloud data, not the CSPs. Backups matter.
3. **Control access:** Adopt a "least privilege" approach when granting access to legally protected or classified data (e.g., GDPR, HIPAA and SOX). Restricting access to mission-sensitive, financial and personally identifiable data reduces the risks of data loss, exfiltration and ransomware.
4. **Update:** Promptly update software applications and leverage secure cloud-native environments. Where possible, automate updates to ensure timely patching and security updates.
5. **Segment:** Partition your network into distinct segments to contain the spread of attacks. "Use modern data protection techniques like software-defined network functions and cloud-native microservices with Kubernetes to lower attack risks," adds Ruffin.
6. **Comprehensive backup and recovery strategy:** Employ the 3-2-1 industry best practices for backup. "For the best data protection, go even further by applying Veeam's 3-2-1-1-0 rule," says Ruffin. Regular immutable backups of on-premises, cloud and tactical edge data can be easily automated. Always test backup and recovery processes to ensure restore point and restore time objectives (RPO/RTO) can be met.
7. **Scan:** Automate anti-virus and anti-malware data scans to run at regular intervals. Scan everything from backups to cloud platforms and on-premises servers.
8. **Modernize:** Newer AIOps platforms use sophisticated algorithms to spot and remediate unusual network, software, container and backup activities or anomalies.
9. **Test:** Objective third-party vulnerability assessments and penetration tests help spot data security weaknesses before they can be exploited.
10. **Share and partner:** By sharing best practices with other agencies, peers and stakeholders, and partnering with industry experts, you can develop more robust defense mechanisms to protect all your data assets.

A comprehensive data protection and recovery strategy is crucial to ensuring agencies remain resilient in the face of ransomware and other cyber threats. To bolster cyber readiness, agencies must rely on strong defensive strategies and tools from partners like Veeam.

To learn more about how Veeam can help your agency improve cyber readiness, visit www. veaam.com

PRESENTED BY NEXTGOV/FCW SPONSORED BY veeam carahsoft.

[1]Veeam 2024 Ransomware Trends Report Executive Summary US Federal Government Edition, https://www.veeam.com/wp-2024-ransomware-trends-executive-summary-us-fed.html