Highlights

Recent Data Breaches

[U-Haul reveals drivers' license details stolen in data breach]
Compromised passwords were used to obtain customer rental contracts going back as far as Nov 2021.

[IRS Data Leak Exposes Taxpayer Information]
The Internal Revenue Service (IRS) has accidentally leaked personal data for approximately 120,000 taxpayers who filed a form 990-T as part of their tax returns.

[Cyber-attack Disrupts Bookings for IHG Hotels]
Hospitality company InterContinental Hotels Group PLC (also known as IHG Hotels & Resorts) says its online booking systems have been disrupted since September 5th after its network was breached.

[Los Angeles School District Hit by Ransomware Attack]
The Los Angeles Unified School District said a ransomware attack over Labor Day weekend took down many of its IT systems, including attendance tracking software, email, storage and other systems provided by Google Workspace. Schools opened as scheduled Tuesday despite the attack.

[Samsung US Says Customer Data Compromised in July Data Breach]
Electronics giant Samsung confirmed a data breach affecting customers' personal information. Samsung said it discovered the security incident in late-July but waited to publicly disclose the incident.

[Russian Streaming Platform Confirms Data Breach Affecting 7.5m Users]
Russian media streaming platform 'START' (start.ru) has confirmed rumors of a data breach impacting millions of users.

[Nelnet Breach Affects 2.5M Student Loan Accounts]
Data for over 2.5M individuals with student loans from Oklahoma Student Loan Authority (OSLA) and EdFinancial was exposed after hackers breached technology services provider Nelnet Servicing.

[DoorDash Discloses New Data Breach Tied to Twilio Hackers]
Food delivery firm DoorDash has disclosed a data breach exposing customer and employee data that is linked to the recent cyberattack on Twilio.

[Uber is Investigating a Potential Breach of Its Computer Systems]
The hacker allegedly social-engineered an Uber employee to get hold of their password by masquerading as a corporate IT person.

Cyber Experts say “Duh” to China’s Accusation the NSA Hacked Its Military Research University

China accused the U.S. National Security Agency (NSA) of cyberattacks against Northwestern Polytechnical University in the city of Xi'an. The National Computer Virus Emergency Response Centre (NCVERC), the counterpart to the U.S. CISA, accused the Office of Tailored Access Operations (TAO), a cyber-warfare intelligence-gathering unit of the National Security Agency (NSA), of orchestrating attacks in China. TAO first became publicly known in 2013 and breaks into networks all over the world to gather intelligence and data. According to the report, "The U.S. NSA's TAO has carried out tens of thousands of malicious cyber-attacks on China's domestic network targets, controlled tens of thousands of network devices (network servers, Internet terminals, network switches, telephone exchanges, routers, firewalls, etc.), and stole more than 140GB of high-value data."

"The U.S.'s behavior poses a serious danger to China's national security and citizens' personal information security. As the country that possesses the most powerful cyber technologies and capabilities, the U.S. should immediately stop using its prowess as an advantage to conduct theft and attacks against other countries, responsibly participate in global cyberspace governance and play a constructive role in defending cyber security." Mao Ning, Deputy Director of the Foreign Ministry Information Department of China.

The U.S. Department of Justice says the Beijing-funded university, Northwestern Polytechnical University, is a "Chinese military university that is heavily involved in military research and works closely with the People's Liberation Army on the advancement of its military capabilities.” Targets like Northwestern Polytechnical University are what most nations would consider “fair game” for government-to-government espionage, prompting reactions of, essentially, “No duh.”

The attack employed cyber weapons designed to siphon passwords, network equipment configuration, network management data, and operation and maintenance data. It also said that the TAO used two zero-day exploits for the SunOS Unix-based operating system to breach servers used in educational

institutions and commercial companies to install the OPEN Trojan. The attacks also included malware "Fury Spray," "Cunning Heretics," "Stoic Surgeon," and "Acid Fox" that are capable of "covert and lasting control" and exfiltrating sensitive information. This attack was launched via a network of proxy servers hosted in Japan, South Korea, Sweden, Poland, and Ukraine to relay the instructions to the compromised machines. The NSA used an unnamed registrar company to prevent the capture of traceable information such as relevant domain names, certificates, and registrants.

Previously, China accused the U.S. of attacks in February, at Pangu Lab via a backdoor Bvp47 that's alleged to have been used by the Equation Group to strike more than 287 entities globally. In April, the NCVERC released a technical analysis of a malware platform, Hive, that was said to be employed by the U.S. Central Intelligence Agency (CIA) to customize and adapt malicious programs to different operating systems, plant backdoors, and achieve remote access.

In this case, the unit appears to have used 41 hacking tools to break into and steal data. One tool, “Suctionchar,” stole account credentials from remote management and file transfer applications to hijack logins on targeted servers. Bvp47, a backdoor in Linux that has been used in previous hacking missions by the Equation Group—another elite NSA hacking team. According to CVERC, traces of Suctionchar have been found in many other Chinese networks besides Northwestern’s.

Yang Tao, the director-general of American affairs at China’s Ministry of Foreign Affairs, published a statement affirming the CVERC report and claiming that the NSA had “seriously violated the technical secrets of relevant Chinese institutions and seriously endangered the security of China’s critical infrastructure, institutions and personal information, and must be stopped immediately.”

The Chinese claims were “highly amusing,” tweeted European security researcher Lukasz Olejnik**.** “I would offer that Beijing seems to be making a recent habit of repackaging old news — suggesting its utility is primarily propaganda,” explains Gavin Wilde, a senior fellow at the Carnegie Endowment for International Peace. “China’s counternarrative to its pervasive cyber activity is not only useful on the domestic front, but coincides with increasing cohesion among Western governments and tech companies in cyber defense and attribution amid Moscow’s war on Ukraine. Even so, having to go to such lengths to explain the logic behind Chinese propaganda is indicative of how slipshod it often is.” Since 2020, the U.S. has accused the Chinese of digitally infiltrating American phone networks, state governments, manufacturing firms, Microsoft, and the private accounts of American journalists.

DHS Announces $1B Cybersecurity Grant Program

The Department of Homeland Security (DHS) announced a $1 billion investment to fund its first-ever cyber grant program tailored specifically for state and local governments to address cybersecurity risks, including identifying key vulnerabilities, mitigating threats and strengthening critical infrastructure. The funds will be allocated over the next four years, with $185 million made available for fiscal 2022. The $1 billion funding is part of a grant program established by the State and Local Cybersecurity Improvement Act, which passed last year as part of President Biden's $1.2 trillion infrastructure package. A separate grant program for tribal governments will be available later this fall.

Eligible applicants have 60 days to apply for a grant, which can be used to fund new or existing cybersecurity programs and will include plans for how they intend to redistribute at least 80% to their local governments, as required by the infrastructure law. Administration officials said the grants will be overseen by the Cybersecurity and Infrastructure Security Agency and the Federal Emergency Management Agency with the goal of awarding funds by the end of the year.

Plans are likely to vary widely from state to state, though a senior DHS official said the federal government has a few objectives, including "effective implementation" of cybersecurity frameworks like the one published by the National Institute of Standards and Technology. CISA is also going be "relying heavily" on its rosters of state coordinators and regional advisers but also promised flexibility.

> "Many state and local governments face unique challenges and deserve support when defending against cyber threats, particularly against nation-states and well-resourced cybercriminals. Threat actors recognize and capitalize on these constraints by exploiting vulnerabilities and limited capacity to recover from devastating cyberattacks."
> Alejandro Mayorkas, Secretary of Homeland Security

The secretary cited several major ransomware incidents over the past few years, including attacks on Atlanta, Baltimore and Tulsa, Oklahoma, as well as last week's attack against the Los Angeles Unified School District.

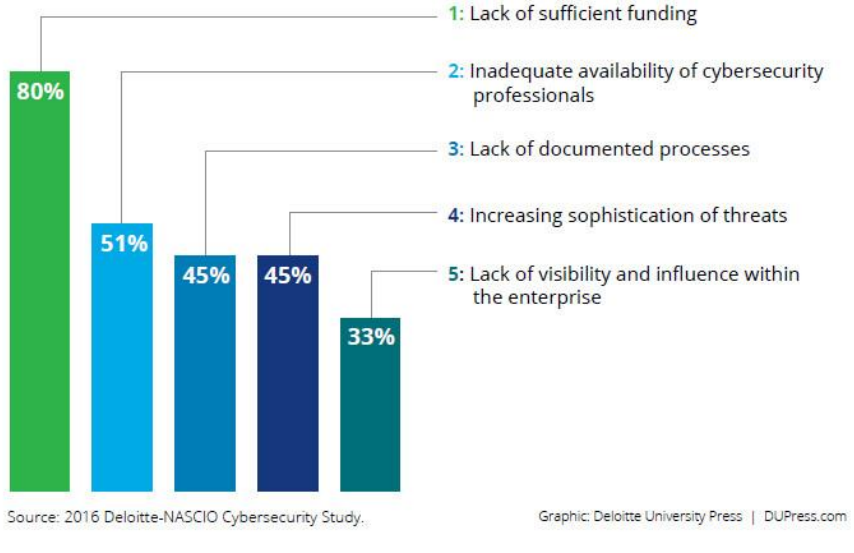
“The goal of this program is to address the enormous challenge that state, local and tribal and territorial governments currently face when defending against cyber threats,” Landrieu said. “With this funding, we are better protecting our most vulnerable communities, ensuring that resource constraints don’t hold them back from developing plans to safeguard their critical infrastructure.”

“Because the law requires jurisdictions to establish cybersecurity plans, we want them to have time to establish those plans,” an official explained. “The expectation is that states would use their first years’ worth of grant funding to develop plans for the remainder of the program, with the final three years’ of funding released once those proposals are approved.”

The FBI and the Cybersecurity and Infrastructure Security Agency released a joint advisory warning that a criminal syndicate known as Vice Society is disproportionately targeting the education sector with ransomware attacks. “School districts with limited cybersecurity capabilities and constrained resources are often the most vulnerable; however, the opportunistic targeting often seen with cyber criminals can still put school districts with robust cybersecurity programs at risk,” the advisory said.

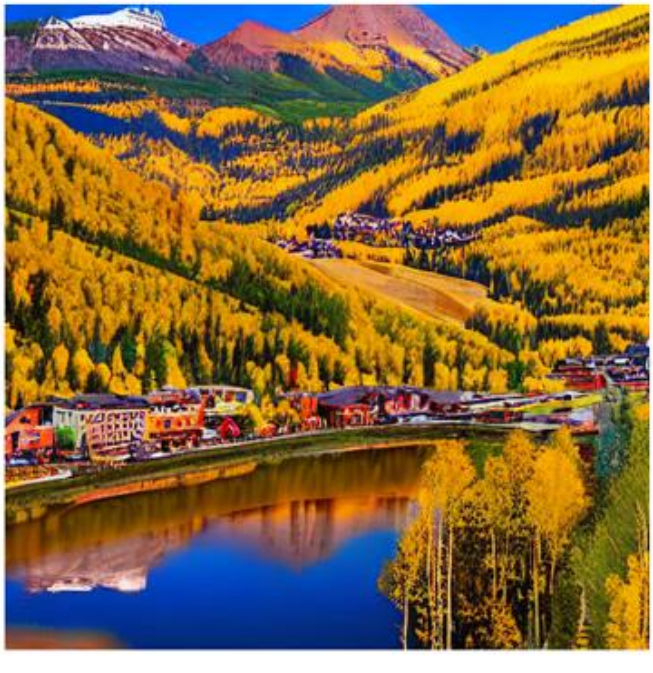
NASCIO and its members have been preparing for the grant program with an acknowledgment that $1 billion over four years, spread across the entire country, is a “drop in the bucket” compared to what states and localities need to defend themselves against a landscape that includes ransomware, foreign governments targeting software vulnerabilities and threats against critical infrastructure facilities.

“Cyberattacks have emerged as one of the most significant threats to our homeland,” said Homeland Security Secretary Alejandro Mayorkas in a statement. “In response, we continue to strengthen our nation’s cybersecurity, including by resourcing state and local communities to build and enhance their cyber defenses,” he added. Landrieu, the White House’s infrastructure lead, said the grant program is designed to “send a market signal from the federal government they need to harden their assets and have an all-hazards approach.” These grants will help address some of the gap between cyber threat and funding for state governments as highlighted below:



AI Generated Images of Colorado Using Stable Diffusion Program

stability.ai



Upcoming Conferences

September 19-20	Industry of Things World, Berlin
September 19-22	NVDIA GTC 2022, Virtual
September 20-22	Dreamforce, San Francisco
September 22-23	Global Cyber Conference, Zurich
September 26-28	InfoSec World, Colorado Springs
September 27-28	International Cyber Expo, London
September 28-29	IoT World, Santa Clara
September 28-30	Spiceworld, Austin, Hybrid
October 3-4	451Nexus, Las Vegas
October 5-6	Evolve, Vegas
October 6-7	Big Data & AI Toronto
October 10-12	ISC Security Congress, Las Vegas
October 11-12	Edge Computing World, Santa Clara, CA
October 11-13	Google Cloud Next, Virtual
October 17-19	Authenticate 2022, Seattle
October 17-20	NAB Show New York, NYC
October 17-20	Gartner IT Symposium/Xpo, Orlando
October 18-20	OCP Summit, San Jose, CA

October 24-27	ICS Cybersecurity Conference, Hybrid/Virtual
November 1-3	NetApp INSIGHT 2022, Virtual
November 13-18	SC22, Dallas
November 16	San Diego Cybersecurity Conference, Hybrid
November 16	Threat Hunting Summit, Virtual
November 18-19	Data Strategy & Insights (Forrester Research), Virtual
November 21-22	Gartner IT Infrastructure, Operations, & Cloud, London
November 28-Dec 2	AWS re:Invent, Las Vegas
December 1-2	AI & Big Data Expo Global, London
December 6	Security Operations Summit, Virtual
December 6-8	Gartner IT Infrastructure, Operations & Cloud, Las Vegas
December 10-14	Edge 2022: International Conf on Edge Computing, Hawaii
December 10-14	Cloud 2022: International Conf Cloud Computing, Hawaii
January 5-8	CES, Las Vegas & Virtual
April 24-27	RSA Conference, San Francisco
May 22-25	Dell World, Las Vegas
June 20-22	HPE Discover, Las Vegas