rubrik

WHITE PAPER

The Impact of Cyber Attacks on US Citizens

The Impact of Cyber Attacks on US Citizens

Ransomware attacks are a national security issue when you consider the disruption of vital services, financial loss, data theft, and even loss of life that these attacks can wreak upon society.

State and local governments continue to be under siege from ransomware and malware attacks, as well as businesses, schools and hospitals. The average cost of a ransomware attack is around $4.5 million, according to recent reports. This cost can be even higher for government entities due to the sensitive nature of the data they manage.

Ransomware is malicious software, also known as malware, that permanently blocks access to a victim's system or data unless a fee, or ransom, is paid. Ransoms are often requested to be paid in hard-to-trace currencies, like Bitcoin. Ransomware is often spread through phishing emails containing malicious attachments or through drive-by downloading, where a user unknowingly visits an infected website and software is downloaded and installed without their knowledge.

According to Gartner, global spending on cybersecurity is expected to be $212 billion by 2025, a 15% increase over 2024. Yet, attacks continue unabated. Several factors contribute to the increase in ransomware and other malware attacks, including the growing sophistication of cybercriminals, the economic motivation for attacks, geopolitical tensions and an increase in vulnerabilities in IT systems and software.

The year 2022 was record-setting for vulnerabilities, with the highest number ever reported: 25,083 vulnerabilities discovered. The next year, 2023, set a new record with a 16% increase, totaling 29,065 vulnerabilities discovered. 2024 is sure to re-set this mark again.

The adversaries know that state and local governments, critical infrastructure, hospitals and schools are our Achilles' Heels. To date, investment and prioritization have been on prevention and compliance, which is not sufficient to stop these attacks. Therefore, the focus should pivot to preparing for such incidents, ensuring cyber resilience and recovery.

Broader Implications

These cases illustrate the widespread and severe impact of ransomware attacks on state and local governments as well as critical services that citizens rely on such as hospitals and schools. Victims face a difficult choice: pay the ransom to regain access or refuse and incur potentially higher recovery costs. The need for robust cybersecurity measures and federal support in combating these sophisticated attacks is more critical than ever. A minimal investment up front can save millions of dollars in potential ransom and/or recovery efforts down the road.

Factors Contributing to the Growth of Ransomware

- **Data Growth:** Data is growing at a pace seven times faster over the next five years.
- **Visibility Issues:** Too much data in too many places without enough visibility.
- **Critical Nature of Data:** Data is like oxygen; you don't think about it until it's gone, and then it's your only thought.
- **High Security Spend:** Despite worldwide spending of $210 billion on security, attacks continue unabated (according to Gartner).

Government Challenges

- **Legacy Systems and Equipment:** Many government entities struggle with outdated systems.
- **Reactive Approach:** A compliance-driven, reactive approach rather than focusing on recovery at scale.
- **Legacy Backup Issues:** Struggling with outdated backup solutions.
- **Adaptation and Urgency:** Slow to adapt and lacking a sense of urgency.
- **Limited Resources:** Limited funding/budget for cybersecurity and technology and a declining workforce with cyber experience.
- **Continuing Resolutions:** Uncertainties associated with a lack of long-term funding.

The Need for Cyber Resiliency and Immutable Backups

In today's digital landscape, the adage "an ounce of prevention is worth more than a pound of cure" holds especially true for cybersecurity. While organizations are often willing to spend tens of millions to recover from ransomware attacks, investing a fraction of that amount in preventive measures can save significant time, money, and stress.

Cybercriminals are increasingly targeting backups. According to a Rubrik Zero Labs study, in 96% of ransomware attacks, attackers attempted to compromise backup systems, and they were at least partially successful in 74% of those attempts. This highlights the critical need for robust backup and recovery strategies.

Best Practices for Cyber Resiliency

- **Immutable Backups:** Ensure that backups are immutable, meaning they cannot be altered or deleted. This prevents attackers from tampering with backup data.
- **Hardened Operating Systems:** Use operating systems that are configured to resist attacks. This includes disabling unnecessary services and ensuring security features cannot be easily disabled.
- **Data Exposure Prevention:** Implement measures to ensure that your data is not exposed to unauthorized access.

Highlighting Ransomware Response Teams

Having a dedicated ransomware response team is essential for dealing with catastrophic events. These teams are trained to manage the complexities of ransomware attacks and can coordinate a swift and effective response.

Cyber Insurance and Budget Considerations

State and local governments should consider cyber insurance as part of their cybersecurity strategy. Allocating budget for cyber insurance can provide financial protection and support in the event of a ransomware attack.

Rapid Recovery with Rubrik

Rubrik provides a powerful solution for rapid recovery from ransomware attacks. With Rubrik, organizations can recover data in minutes or hours, not days, weeks, or months. This quick recovery capability is crucial in minimizing downtime and maintaining business continuity.

Backups are an essential way for an agency or organization to defend against ransomware. Advanced ransomware is now targeting backup, though, modifying or completely wiping them out. Hence, the growing importance of cyber resiliency and the need for faster ransomware recoveries from immutable backups—backups that cannot be compromised.

The Rubrik Approach

Recovering from a ransomware attack can be complex and time-consuming. Identifying the scope of the attack, locating the most recent clean data, and recovering quickly can be a daunting task, especially while ensuring backups have not been deleted or encrypted.

With Rubrik, all data is stored in an immutable format, preventing ransomware from ever accessing and encrypting backups in the first place. In the event of an attack, Rubrik provides fast recovery to the most recent clean state, granular visibility into the scope of the attack, and can alert an agency to unusual behavior by leveraging machine learning.

LEARN MORE ABOUT FASTER RANSOMWARE RECOVERY FROM BACKUPS THAT CANNOT BE COMPROMISED

ABOUT RUBRIK

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information, please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.

Appendix

The Impact of Ransomware Attacks:
State and Local Government, Businesses, and Hospitals Under Attack

ALABAMA
City of Birmingham

On March 6, 2024, hackers accessed the city of Birmingham's network, disrupting various computer systems. The disruption significantly affected the city's budget process, forcing manual data entry and delaying the preparation of the 2025 fiscal year budget.

Meanwhile, on June 17, 2024, the Alabama State Department of Education blocked a ransomware attack. However, criminals still managed to steal several documents from compromised servers and disrupt some services before they were stopped.

CALIFORNIA
Los Angeles Superior Court

In July 2024, the Los Angeles County Superior Court was hit by a ransomware attack that shut down the nation's largest trial court system. The LA County Superior Court is the largest unified superior court in the United States, serving the county's 10 million residents over 36 courthouses. The attack affected the court's website, case management systems, and My Jury Duty Portal, forcing the closure of all courthouses for two days as a team of consultants, vendors, and law enforcement worked to get systems back online.

CALIFORNIA
Statewide Health Entities

In November 2023, a ransomware attack caused Tri-City Medical Center in Oceanside, California to divert ambulance traffic to other hospitals. The attack caused widespread disruption, shutting down the majority of the hospital's emergency services and forcing the hospital to declare a state of emergency. That attack impacted the personal identification information of 108,149 people. It took nearly eight days for the hospital to restore its systems. Healthcare providers in San Diego County have frequently faced severe cyberattacks. In 2021, a ransomware attack shut down much of the Scripps Health network, crippling electronic healthcare record access and forcing bedside workers to return to paper record keeping. Access to medical imaging was also severely impacted. The financial statements indicated that the attack cost the hospital $113 million in lost revenue, in addition to millions spent on settlements with affected patients. Meanwhile, in the summer of 2021, UC San Diego Health also reported that it suffered a data breach that resulted in the potential release of protected information.

MARYLAND

City of Baltimore

Baltimore City has experienced multiple ransomware attacks. In May 2019 attackers locked city employees out of their email accounts and prevented citizens from accessing essential services for two weeks. The city refused to pay the ransom, resulting in tens of millions of dollars in recovery costs. This was Baltimore's second ransomware attack in about 15 months, when the 911 dispatch system was hit by a cyberattack, highlighting the persistent threat and the high costs of recovery.

MISSISSIPPI

Singing River Health System

In August 2023, a ransomware attack on the Singing River Health System affected about 895,204 individuals. For several days, the attack incapacitated IT systems, including the hospital's electronic medical record system, disrupting its operations. The initial report to the Health and Human Services Office for Civil Rights (HHS OCR) stated a much smaller number of affected individuals, later revised significantly upwards. The compromised data included names, dates of birth, addresses, Social Security numbers, medical information, and health information.

NEBRASKA

Winnebago Public Schools

In October 2023, Winnebago Public Schools suffered a cyberattack. The school district dismissed students from class early and canceled classes altogether on October 23 due to the attack. In addition to locking down school computer systems, the ransomware group Interlock said it stole 223 GB of data from the district containing personal data of employees and students. It posted images of the allegedly stolen data to prove its claim.

NEW YORK

Legislative Bill Drafting Commission

According to a state comptroller's report released in 2024, New York ranks third nationwide for the most ransomware attacks. Attacks on critical infrastructure nearly doubled within the first six months of 2023. On April 17, ransomware hackers attacked the Legislative Bill Drafting Commission — the primary system used to print the final version of Governor Kathy Hochul's state budget.

According to Hochul, the hack, widely reported at the time, derailed the bill drafting process and forced the commission's staff to temporarily revert to an antiquated 1994 computer system as they finalized the state budget. In addition, the hackers obtained driver's license numbers, credit card information, and Social Security numbers.

NORTH CAROLINA

Bladen County

A cyberattack in 2023 on Bladen County, North Carolina, forced officials to call in the state's National Guard for assistance. The attack, which went beyond information theft, led to the involvement of the North Carolina Joint Cybersecurity Task Force to secure the county's servers. North Carolina is one of the few states that have banned government entities from paying ransoms, providing a detailed playbook for handling such attacks.

RHODE ISLAND

RIBridge

On December 5, 2024, a ransomware attack on Rhode Island health services exposed the personal data of hundreds of thousands of patients. Hackers threatened to release information about Rhode Islanders connected with RIBridge, the state's health and social services system that suffered the cyberattack. Deloitte, the state's IT vendor, informed the state that there was a significant security threat to the RIBridge system.

The vendor told state officials that cybercriminals had likely obtained files containing personally identifiable information, such as names, addresses, dates of birth, Social Security numbers, and certain banking information. State officials took the system offline to address the cybersecurity threat and restore operations.

SOFTWARE SOLUTION PROVIDER

CDK Global

In June 2024, a cyberattack on CDK Global, a software provider for car dealerships, disrupted thousands of dealerships across North America. The attack caused operational disruptions for customers, including delays and difficulties tracking orders, sales, and customer interactions. Dealerships reverted to manual processes, such as handwriting orders, to continue sales. Some dealerships also used alternative routes to provide sales and service support. The attack resulted in millions of dollars in losses for dealerships.

SOUTH DAKOTA

Statewide Local Governments

Ransomware attacks increasingly target municipalities nationwide, and South Dakota is not exempt. According to the Center for Internet Security, 2023 saw a 51% surge in ransomware incidents targeting state and local governments during the first eight months of the year compared to the same period in 2022. Some ransomware and cyberattacks on local government in South Dakota include Brown County, which suffered a cyberattack in 2021 affecting services, and the city of Sioux Falls, which sent two electronic payments to someone impersonating a vendor in 2018. Hutchinson County was hit by a ransomware attack in 2019, which temporarily shut down accounts that contained receipts and records for $4 million in county business, underscoring the pressing need for enhanced cybersecurity measures.

TEXAS

City of Dallas

Government agencies in Texas have been under attack for years. In May 2023, a ransomware attack on the city of Dallas compromised the data of 30,000 people, including some Social Security numbers and other sensitive data. A significant cyberattack campaign launched by the REvil ransomware group in 2019 impacted Texas government agencies and municipalities, forcing the state to declare a state of emergency due to the widespread disruption caused by the coordinated attack on at least 23 cities, with potential impacts on many more. Although the perpetrators were eventually indicted and arrested, the effects of this campaign are still being felt by both individuals and businesses across Texas, demonstrating the lasting repercussions of older cyberattacks.

TEXAS

UMC Health System

In September 2023, the UMC Health System, which operates University Medical Center, faced a severe ransomware attack. As the only Level 1 trauma center within 400 miles, the hospital had to divert ambulances with emergency and non-emergency patients to other local hospitals after disconnecting its IT network. John Riggi, the American Hospital Association's national advisor for cybersecurity and risk, highlighted the gravity of the situation by calling it a "national security issue." He emphasized the life-threatening risks when cyberattacks target essential trauma centers and urged federal intervention like the government's counterterrorism efforts.

VIRGINIA

VA Gas Stations & VA's Division of Legislative Automated Systems

On May 7, 2021, the Colonial Pipeline company was targeted by a ransomware cyberattack that disrupted their operations significantly. The attack forced the company to shut down a gasoline pipeline that services most of Virginia's gas stations, leading the governor to declare a state of emergency. Later that year, Virginia's Division of Legislative Automated Systems was hit by a ransomware attack during a legislative session, causing panic and significant disruptions. This incident underscored the vulnerability of governmental operations to cyber threats.

WASHINGTON

Statewide Court Systems

In early November 2024, a cyber intrusion caused outages within court systems across Washington. Based on the serious threat to the Washington Courts network and in consultation with the Chair of the Judicial Information Systems Committee, the Administrative Office of the Courts (AOC) decided to shut down the Judicial Information System and completely isolate the Washington Courts network from the internet. The outages affected courts in the counties of Thurston, Monroe, Renton, Puyallup, Bainbridge, King, Pierce, Whatcom, and Lewis, as well as municipal courts in several cities. Over two weeks, AOC staff worked to rebuild

key components of the Washington Courts network in a secure and sterile environment. Interestingly, forensic analysis revealed that this was not a targeted attack, as the original malware infection came from a site not related to the State of Washington or any courts. AOC expects recovery and restoration efforts to continue at least through the end of 2024 as significant work remains to be accomplished to fully restore all services, including access to the Appellate Court Document Portal.

WEST VIRGINIA

Berkeley County Schools

On January 4, 2024, a cyberattack on the municipality of Beckley, West Virginia, caused a security breach within the city's computer network, which helps govern a population of 17,000 people.

In February 2023, a cyberattack affected Berkeley County Schools' internet and phone services, forcing 20,000 students to miss classes. The school warned students and parents that the attackers may have accessed school data but did not know if any personal data was breached.

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

wp-the-impact-of-cyber-attacks-on-us-citizens / 20250304