The State of Cybersecurity in America
Managing business risk is top of mind for any state Chief Information Officers (CIO) and is a formidable challenge given the ever changing threat landscape. Having worked extensively with state and local governments for the past decade, I fully understand the importance of addressing the business risk that comes with maintaining cybersecurity. The potential impact of a security breach is significant and can have far-reaching consequences for all parties involved. Hackers go after data-rich targets regardless of sector, emphasizing the need to be one step ahead by utilizing proactive security solutions. It can seem like an uphill battle securing a state organization with a diverse IT infrastructure, limited resources, legacy systems, and constantly emerging threats. That’s where Securin comes into play as a technology-enabled cybersecurity solutions company. The Securin platform has become a valuable tool that provides Chief Information Security Officers (CISOs) and CIOs answers to critical questions such as:

1. How is my state at risk of cyberattacks?
2. Are there vulnerabilities within my state that could compromise data security and privacy?
3. What immediate steps can I take to secure my assets?

In this report, we examined dangerous exposures and vulnerabilities that exist in US government domains and the risks they pose to the data security of critical infrastructures. Through this report, the Securin team outlines actionable recommendations that can help state entities fix exposures and increase their security posture.

Thanks,
Ram Movva
CEO & Co-Founder, Securin
Introduction

In the last few years, there has been a strong upswing in cyberattacks on US government entities, State and Local government and Education (SLED) organizations, and public sector enterprises. According to recent reports, cyberattacks on government entities increased by 95% in 2022. They are prime targets for attackers as they possess massive amounts of personal and sensitive data like civil records, financial data, and national security intelligence. Recently, the City of Dallas was attacked by Royal Ransomware, which compromised several local government entities and crippled essential services, including the Dallas City Police and other public-facing systems.

In 2020, 90% of enterprises implemented remote work capabilities without addressing critical security issues. Consequently, 25% of enterprises reported cyberattacks. - TechBeacon

In 2022, 106 US state and local government entities reported ransomware attacks; 25% of these attacks resulted in data theft. - Security Intelligence

This rapid growth of cyber attacks can be attributed to several factors. Including how the COVID-19 pandemic increased the need for remote work, which led to a significant rise in remote system access and the expansion of attack surface. Furthermore, the maturing of Ransomware-as-a-Service (RaaS) into a full-blown industry has made it easy for criminals to mount attacks using out-of-the-box ransomware tools. Along with that, cyber threat actors now serve as Initial Access Brokers (IAB), offering ransomware and gangs state-sponsored cybercriminals convenient access points to their desired targets. The commercialization of cybercriminal activities spotlights the need for security teams to have a hacker’s view

Given these evolving threats, US government entities must adopt a proactive approach to attack surface management. By being acutely aware of their organization’s attack surface and taking proactive steps to secure it, CIOs and CISOs can significantly mitigate the risk of cyberattacks, protect critical data, and safeguard the public’s trust. The battle against cyber threats is ongoing, demanding constant vigilance and a commitment to maintaining a resilient and well-protected digital ecosystem.
Executive Summary

Securin experts conducted passive scans of the 50 United States' domains and State departments, revealing crucial insights into the reasons behind their constant attacks and what made them vulnerable to hackers. The results are as follows:

- **US States domains are hosting numerous high-risk services, thereby exposing valuable assets to the risk of exploitation.**
- **A significant number of internal non-production systems are accessible from the internet, creating easy opportunities for infiltration by hackers.**
- **Several domains contain assets with unpatched high-risk vulnerabilities known to be previously exploited by ransomware gangs.**

These compelling findings make this report essential reading, especially for CISOs and CIOs who are responsible for managing these domains. It offers crucial insights into the dangers posed by these exposures and provides actionable next steps for remediation.

Key takeaways for US state agencies to address these security concerns are to undertake diligent remediation efforts entailing:

1. **Strong Security Controls:** Apply strict access control measures to open ports. Use firewalls, network security groups, or access control lists (ACLs) to restrict inbound and outbound traffic to authorized sources and destinations.

2. **Attack Surface Management:** Continuously perform attack surface scans to discover and address critical exposures. This proactive approach helps identify potential vulnerabilities and areas of concern, allowing for timely remediation and reducing the overall attack surface.

3. **Prioritize Vulnerabilities:** Assess vulnerabilities based on their criticality and potential business impact. Prioritize patching and remediation efforts to address high-risk vulnerabilities promptly, reducing the window of opportunity for attackers to exploit them.
What Does This Mean for You?

High-Risk Services

High-risk services are critical services exposed to the internet that present a clear gateway for hackers to enter a network. When we scanned the US state domains, we discovered 8 million addressable IPs and 119,000 instances of high-risk services that adversaries could easily exploit. This includes Remote Desktop Protocol (RDP), File Transfer Protocol (FTP), Secure Shell (SSH), and databases (MySQL, MongoDB, IBM DB2, MariaDB, and PostgreSQL) open to the internet. RDP, FTP, SSH, and databases are extremely critical to organizations. If exposed to the internet, attackers can exploit them to gain unauthorized access to the system, leading to data theft, denial-of-service (DoS) attacks, and even system compromise.

Remote Desktop Protocol (RDP) allows employees to access their office desktop computers remotely through another system. Predictably, RDP usage soared during the pandemic lockdowns. Our investigation revealed 1,800 instances of open RDP exposures across all US state domains, posing a significant security threat to state entities and the data on these domains. A survey published in Security Week revealed that 44% of security breaches in enterprises occurred because of RDP exposures, and according to a recent investigation by a cyber insurance company, exposed RDP was listed as the most popular attack vector used to gain access to victims’ networks.

File Transfer Protocol (FTP) is a widely used network protocol that facilitates the transfer of files between a client and a server over a computer network. With FTP, users can easily upload, download, and manage files, enabling seamless file transfers across different systems. Despite its ease, the standard FTP is not encrypted and leaves data open to breaches. There are more secure alternatives to FTP like FTPS, HTTP, or SFTP. In our research...
we found 2,782 instances of open FTP ports across all US state entity domains. An open FTP port can cause massive damage as seen when MedEvolve, a healthcare technology and services company, misconfigured its FTP server and exposed the personal data of 205,000 patients. Most security breaches like this are due to internal misconfigurations or neglected patch updates.

**Secure Shell (SSH)** is a secure protocol used for remote access that provides a secure and encrypted communication channel between two devices. Leaving the SSH service open and accessible to the internet without proper security measures allows hackers to use automated tools to scan for open SSH ports and use brute-force techniques to gain unauthorized access to systems. **We discovered more than 3,400 instances of SSH in all US state domains.** If left open the assets on these domains are exposed to significant risk.

**Databases** exposed to the internet without proper security measures in place risk the confidentiality and integrity of the data stored within them. **We discovered over 3,700 instances of exposed databases across all US states.** Of the many database exposures that have led to notable data breaches, the most recent case involved the Toyota Motor Corporation, where a misconfigured database exposed vehicle location data for 2,150,000 customers.

Knowing the cybersecurity posture of your organization is top of mind for every CIO and CISO. Timely and accurate information on threats, vulnerabilities, and the state of your own environment is vital to any organization's endeavors to defend against data and system breaches, respond to threats, and maintain cybersecurity operations. As cyber threats continue to evolve, the State of Arizona collaborates with all industries and all levels of government to share intelligence data, best practices, learn from past events, and continue to find new ways to protect the entire state from potential attacks.
# Recommended Actions for High-Risk Services

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Business Impact</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credential theft via open Remote Desktop Applications (RDP) and data theft through the exposed database</td>
<td><strong>Credential and Data Theft</strong>&lt;br&gt;Open RDP ports may lead to credential theft and ransomware attacks and cause reputational harm and disruption of critical state services.&lt;br&gt;Databases exposed to the internet without ample security allow hackers to steal sensitive information, modify or delete data, deploy ransomware to encrypt files, and distribute malware to other systems on the same network.</td>
<td><strong>Open RD Ports</strong>&lt;br&gt;- Implement Multi-Factor Authentication (MFA)&lt;br&gt;- Adopt complex passwords&lt;br&gt;- Restrict RDP usage&lt;br&gt;- Use RDPs within a Virtual Private Network (VPN)</td>
</tr>
<tr>
<td>Data interception via unencrypted File Transfer Protocol (FTP) networks</td>
<td>Lack of data encryption while transferring data can provide an entry point for attackers to infiltrate the FTP network, leading to data loss and malware distribution.</td>
<td><strong>Exposed Database</strong>&lt;br&gt;- Use strong authentication&lt;br&gt;- Update access controls&lt;br&gt;- Apply security patches and updates&lt;br&gt;- Ensure proper configuration of security settings&lt;br&gt;- Restrict database access to authorized personnel only</td>
</tr>
<tr>
<td>Unauthorized access via open Secure Shell (SSH) services</td>
<td>Hackers often scan for open SSH ports and use brute-force to gain unauthorized access, after which attackers execute commands, install malware, and compromise the stability of the entire network.</td>
<td><strong>Use strong passwords or public-key authentication&lt;br&gt;- Disable root login&lt;br&gt;- Limit access to specific IP addresses&lt;br&gt;- Use firewalls or intrusion prevention systems (IPS) to monitor and block suspicious activity</strong></td>
</tr>
</tbody>
</table>
Exposed Non-Production Systems

A non-production system is an environment separate from the live production environment, used for testing, development, and staging purposes. Attackers have long used exposures in non-production systems to exploit their targets. These systems do not have adequate security controls making them easy to infiltrate, which leads to data breaches, reputational loss, and financial damage to enterprises and entities alike.

Breaches like this can happen to any enterprise, as it did to Uber in 2018. Uber’s software engineers were involved in the development and testing of software that had the capability to connect to the cloud. However, due to inadequate access controls, intruders were able to exploit Uber’s development environment to access backup databases containing information about Uber users and drivers.

In our research, Securin ASM discovered 11,000 non-production systems connected to the internet in US state department domains. They consisted of 59% development environments, 33% testing environments, and 8% User Acceptance Testing (UAT) assets, all exposed to the internet.

The thousands of non-production system exposures in state domains pose a significant risk. Most of these exposures were seen in the Health Services, Economic Services, and Education departments. It is strongly recommended that the respective security teams conduct periodic vulnerability assessments to identify and promptly address these vulnerabilities and misconfigurations.

By following industry best practices, prioritizing critical vulnerabilities, and establishing ongoing vulnerability management, IT and security teams can enhance the security posture of these systems, thus safeguarding sensitive information while reducing the likelihood of security breaches and unauthorized access.
### Recommended Actions for Exposed Non-Production Systems

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Business Impact</th>
<th>Remediation</th>
</tr>
</thead>
</table>
| Infiltration through exposed non-production systems | The risk of unauthorized access, data theft, data exposure, and cyberattacks is high. | - Segregate the network to minimize exposure  
- Implement access control and limit access  
- Use multi-factor authentication  
- Monitor network activity and system logs  
- Perform regular vulnerability scans and remediation |
High-Risk Vulnerabilities with Public Exploits

High-risk vulnerabilities are characterized by their potential to inflict substantial harm on an organization's systems, data, or reputation. Multiple state government entities have been compromised due to high-risk vulnerabilities, as evidenced by recent incidents. In October 2022, a CISA advisory revealed that a US military contractor's enterprise network was compromised using high-risk Microsoft exposures. Attackers have also repeatedly targeted government entities using the Print Nightmare (CVE-2021-34527) vulnerability in the Windows Print Spooler service, leading to an emergency directive from CISA to disable the service on all federal agency networks.

Our scans uncovered 18 high-risk vulnerabilities classified as Remote Code Execution (RCE)/Privilege Escalation (PE) exploits existing in assets within the US state domains. One vulnerability in PHP is currently being exploited by NextCry ransomware, and 13 of the vulnerabilities are actively trending in hacker chatter. These RCE/PE vulnerabilities are found in various software, including Microsoft Internet Information Services (IIS), Python, WordPress, Apache HTTP Server, PHP, OpenSSL, OpenBSD, OpenSSH, and Drupal. The worst-affected vendors, with three vulnerabilities each, are Microsoft and WordPress.

The US government lost $70 billion to ransomware attacks from 2018 to 2022.

- Comparitech
### Recommended Actions for High-Risk Vulnerabilities with Public Exploits

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Business Impact</th>
<th>Remediation</th>
</tr>
</thead>
</table>
| Exploitation of high-risk vulnerabilities     | Risk of unauthorized access to sensitive information, disruption of critical services, incidents of downtime, and performance issues | - Prioritize high-risk vulnerabilities for patching  
- Follow industry-standard frameworks, such as OWASP Top 10, to identify and mitigate vulnerabilities  
- Continuously run attack surface scans to identify and remediate critical exposures and vulnerabilities  
- Monitor and mitigate end-of-life (EOL) products to upgrade or decommission them |
Risk of Ransomware Attacks

From a ransomware perspective, our analysis revealed that US state domains are at high risk of ransomware attacks. **State domains contained numerous ransomware-associated vulnerabilities with over 600 vulnerable assets.** The Securin ASM platform also identified 1,990 instances of ransomware exposure to notorious groups, such as NextCry and Ryuk, which have been targeting US government entities since 2020.

Almost all US state departments are at risk of ransomware attacks; however, the Education, Health Services, and Administration state departments had the most assets with ransomware-associated vulnerabilities. When we correlated this with the recent Internet Crime Report released by the FBI, we observed that the majority of complaints received by the FBI belonged to Health Services and Administration. A research report revealed that government entities lose an average of 17 days in downtime trying to recover from a ransomware attack.

Promptly addressing ransomware-associated vulnerabilities mitigates the risk of exploitation and prevents potentially devastating consequences caused by ransomware incidents. It is imperative for all state agencies to train employees to be aware of phishing scams and recognize suspicious activity to mitigate the human risk.

**Recommendations for Risk of Ransomware Attacks**

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Business Impact</th>
<th>Remediation</th>
</tr>
</thead>
</table>
| Exploiting vulnerabilities to mount ransomware attacks | Exposure of sensitive information in the public domain, suspension of critical services, disruption of operations, loss of trust, reputation, and financial loss | - Prioritize high-risk vulnerabilities for patching  
- Follow industry-standard frameworks to identify and mitigate exposures  
- Continuously run attack surface scans to identify and remediate critical vulnerabilities  
- Monitor products for upgrade or decommission |
Other Noteworthy Findings

Apart from these high-risk findings, Securin ASM also discovered:

- 23,000 leaked credentials belonging to US state domains with the potential to be exploited for phishing attacks
- 274,000 compromised IP addresses accessing state domain URLs and exposed third-party risks
- Unpatched instances of CISA's Known Exploited Vulnerabilities in violation of CISA directives for all US federal agencies

Conclusion

Our findings reveal that all US state government domains are in danger from high-risk services, exposed non-production systems, high-risk vulnerabilities, and ransomware attacks. Exposures like these can be targeted by threat actors and need prompt remediation to keep data secure.

Enterprises need better visibility into their attack surface to fix exposures that could be potentially exploited by attackers. We recommend implementing strong authentication measures, segregating networks, incorporating better security controls, limiting access, patching high-risk vulnerabilities associated with ransomware and threat groups, and taking frequent backups. Security teams in US state entities are encouraged to consider adopting continuous attack surface management to discover unknown assets and their exposures and run vulnerability management programs to manage all vulnerabilities in known assets. Additionally, US states keen on enhancing their cybersecurity protocols can consider taking proactive measures such as penetration testing to test their defenses against malicious intrusion.

Get an exclusive Exposure Report!
Contact us to learn how to keep your State safe.

Securin

Message from Leadership
Introduction
Executive Summary
High-Risk Services
Exposed Non-Production Systems
High-Risk Vulnerabilities with Public Exploits
Risk of Ransomware Attacks
Conclusion

Contact us to learn how to keep your State safe.
info@securin.io
securin.io