Mitigating Cyber Threats: A Roadmap for Secretaries of State

CIVIX VICE PRESIDENT OF TECHNOLOGY SHARES CYBER RESILIENCE BEST PRACTICES

By: Calvin Simmons, *Vice President of Technology, Civix*

Cyberattacks are on the rise, growing exponentially year over year. The threat level now is especially high due to Russia's war in Ukraine. As such, cybersecurity authorities of the U.S. and allied nations released a joint Cybersecurity Advisory (CSA)[1] in April warning of an increased risk of malicious cyber activity by Russia and aligned criminal organizations.

Even during "regular" circumstances, though, state and local governmental entities are appealing soft targets to nefarious actors, if not for financial gain, then for the potential to disrupt the American way of life. The threat is especially high for U.S. secretaries of state (SOS), which are responsible for systems critical to the nation's democracy and economy. Furthermore, while SOS integration of modern technology has improved these systems, it has also made them more vulnerable to malicious cyber activity.

During the 2016 presidential election, Russia targeted election officials in every state. While U.S. systems are better defended today, nefarious actors may still seek to capitalize on American's low confidence in election integrity to further shake confidence in election results, especially in the national midterm elections in November. Likewise, business services systems are vulnerable to fraudulent filings.

Thus, SOS should heed the CSA, which urges authorities "to prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity." The Cybersecurity & Infrastructure Security Agency (CISA) provides recommended hardening actions, and this paper strives to share principles upon which strong cybersecurity programs are built. These should be adopted by SOS to create greater "cyber resilience" – the ability to prepare for, respond to, and recover from cyberthreats and attacks.

Best Practices for Cybersecurity

NIST STANDARDS

The National Institute of Standards and Technology, part of the U.S. Department of Commerce, develops cybersecurity standards, including the NIST Cybersecurity Framework (CSF)[2]. While only mandatory for U.S. federal government agencies, SOS should look to the Framework for guidance and to determine which activities are most important.

DEFENSE-IN-DEPTH

Just like a castle provides multiple lines of defense with moats and walls to protect the keep, a Defense-in-Depth (DiD) approach to cybersecurity layers defensive mechanisms to protect valuable data. If one such mechanism fails, then another is in place to thwart an attack. These overlapping layers of defense increase the security of a system as a whole against different attack vectors. Layers deployed by solution providers include tiered networks with default deny/explicit allow only, endpoint detection and response, robust Identity and Access Management (IAM), three complementary firewalls, secure cloud environment, and a FedRAMP High hosting environment. These stacked protections create a deeply layered security posture.

ZERO TRUST ARCHITECTURE

Leveraging a Zero Trust approach, SOS can make their systems more secure through strong authentication models, network segmentation, and outermost layer protocols, among others. These tactics help prevent any user or device, inside or outside a network, from accessing an IT system until authenticated and continuously verified.

A Zero Trust approach includes leveraging a robust IAM program that encompasses the identification, authentication, and authorization of individuals to have access to resources.

Partnering with top credit agencies can help rapidly authenticate the identity of applicants based on definitive data sources, and Identity Assurance is met when it is determined that an applicant is who they claim to be. If they meet this threshold, then they become a registered user with login credentials. Varying levels of authentication rely on additional data that is difficult to produce, except by that specific person, to re-enter the system with those login credentials.

AUTOMATED PROVISIONING

The first key tenant of IAM, automated provisioning facilitates end-to-end automation based on specifications, policies, and analytics – without the need for human intervention and opportunities for human error. User identities and roles are automatically created. In addition to activating services for users, it can also remove user access to systems and data.

Seeing a wave of fraudulent business registration filings, automated entity security techniques have been created, allowing admins to create online user accounts and roles. An "owner," the top-ti-

er user role, can assign users a variety of privileges, each with varying levels of filing and viewing permissions. The entire process is performed online by users without any need for the SOS to be involved. This type of automated provisioning is an important next step in ensuring cybersecurity.

CONTINUOUS MONITORING

Key to cyber resilience is 24/7/365 monitoring. Partnering with around-the-clock security monitoring services ensure preventive and ongoing real-time operational measures. Event data is collected, correlated, and monitored continuously in a security information and event management (SIEM) technology for detection of potential security incidents, which triggers appropriate responses to ensure every threat is managed. This real-time monitoring and response capability is essential for SOS, especially during election voting and reporting.

BEST-IN-BREED SECURITY TOOLS

By stacking the software tools that are each best at the discrete problem it solves, SOS can better manage data in a safe and effective manner. This best of breed approach also allows SOS to do more with their limited budgets. By integrating leading security software tools, SOS are benefitting from the significant investments vendors have made in these products. For example, building a FedRAMP High compliant hosting environment would likely not be attainable for a state agency, but migrating to a FedRamp certified cloud service is not only within reason, it should be considered foundational to success.

SECURE CLOUD ENVIRONMENT

Secure cloud environments are a clear best practice for SOS. They provides dynamic elasticity, scalability, redundancy and improved cybersecurity. Cloud hosting further enables a high level of security, speed, and transparency that is essential to boosting constituent and voter confidence.

CONCLUSION

Because the risk landscape is ever evolving, SOS must continuously work to create cyber resilience. Grounded in best practices, a security program can be nimble and customized to meet SOS unique needs and mitigate new threats.

LEARN MORE

Civix is a trusted software provider on a mission to transform the public sector.
For more information, visit gocivix.com or contact solutions@gocivix.com and 888-GOC1V1X.

[1] Source: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a

[2] Source: https://www.nist.gov/cyberframework