Arizona Cybersecurity Team Recommendations

December 31, 2019

Executive Summary

The Arizona Cybersecurity Team (ACT) is providing seven recommendations to improve cybersecurity in our State. The recommendations focus on: improving information sharing; strengthening incident response; enhancing consumer protections; centralizing efforts to increase awareness of cybersecurity threats; decreasing risk; helping Arizonans better protect themselves online; and improving our educational programs as part of increasing the talent pipeline, to better prepare our future workforce and defend our organizations.

Following the Governor's Executive Order creating the ACT, the team broke down previous barriers of communication within the community and enhanced collaboration to move cybersecurity forward in our State. This was accomplished by proactively and regularly bringing together leaders in this field to work together. Quarterly threat briefings from the State's Chief Information Security Officer allowed for a better understanding of the threats, as well as greater transparency between elected officials, private sector representatives, academics, law enforcement, statewide officials, and the public.

In order to become a nationwide leader, Arizona should focus on taking actions that make it more difficult for criminal hackers to succeed. Throughout ACT meetings, this has been referred to as “increasing the cost to the hacker.” Cybercrime jeopardizes Arizona citizens’ public safety, and the state has an opportunity to lead efforts which make cybersecurity a priority. The State can accomplish this by increasing partnerships with law enforcement and prosecutors to hold criminal hackers accountable.

The continuation of a formal team is not recommended in this proposal; however, the team members will continue to help implement the opportunities identified. The relationships built by the team will continue to keep the momentum moving forward, but the goal is to broaden the work that has begun to include the entire state. In the future, an increased focus placed on enhancing existing relationships with the private sector will push innovative solutions and strengthen information sharing.

The recommendations included in this report are not ordered by priority. The appointed ACT team members were given authority to create sub-committees, which brought in additional private sector input and expertise. Through a single website, a speaker’s bureau, and expanded engagement with our educational partners, Arizona will be better-positioned for the evolving challenges in cyberspace.

Recommendation #1: Improve the Information Sharing for Public and Private Sector Collaboration

Problem: Currently, cyber information in Arizona is not being collected, analyzed, or shared as efficiently as necessary. Two main contributing factors to this problem are the lack of a central communication point for cybersecurity information and the absence of proper infrastructure to ensure the secure sharing of information between industry partners. An effective and efficient working relationship between critical public- and private-sector partners will create a more secure environment for the entire State. We need to ensure we have a coordinated effort that results in consistent and timely information channels between crucial Arizona businesses and agencies.

Solution:
A. The state should create a central communication point for cybersecurity information in Arizona to collect, analyze, and disseminate cybersecurity information across different sectors and levels of government.

B. The state should maintain secure communication channels that are appropriate to efficiently share sensitive and classified information.

Background: Every day, the number of cyber-attacks attempted and the amount of user data targeted increases, resulting in an exponential increase of sensitive and classified information. To better serve and protect Arizonans, this information must be communicated securely and quickly between different agencies and sectors.

The information hub mentioned above will be utilized by federal, local, and state partners, as well as private sector entities, including the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), Law Enforcement and Public Safety partners, Information Sharing and Analysis Centers (ISACs), Cyber Emergency Response Teams (CERTs), and others which provide critical infrastructure.

Maintaining secure communication channels will require continued monitoring of the state's networks, cyberinfrastructure, and security controls to appropriately secure the information being shared from those trying to access it maliciously. (e.g., email encryption, protected chat room platforms).

Recommendation #2: Increase the Speed of Information Sharing

Problem: Currently, it is taking too long to share sensitive information that could potentially protect both the public and private sectors in Arizona. The state lacks means to report and share valuable information past those who "need to know" in a timely manner.

Solution:
A. Speed up information sharing through enhanced use of the state's fusion center and open-source briefings:

1. Increase AZ Cyber Briefings - ongoing, intermediary intelligence and situational briefings provided to verified cyber-industry personnel
2. Offer multiple levels of briefings and schedule regular briefings for those with clearances
3. Leverage InfraGard - The Public-Private information-sharing entity led by the FBI
4. Leverage national briefings - look into providing national/federal briefings to more industry personnel with appropriate clearances

Background: This recommendation requires little to no cost for the coordination of briefings. The lift would be in coordinating the different/recurring briefings, and working with intelligence officials to redact information to ensure any classified information is not given out to those without the appropriate clearance.

In many situations, intelligence-sharing is slowed because it is classified. Classified information is continuously criticized for either not being shared rapidly enough, or not being kept private enough. Often, the classified part of intelligence is the "who" or attribution of a situation, and not the "what" of the information. However, much of the actionable part of the information is in the "what" of a situation and not the "who." Therefore, much of the information can go from being classified to "For Official Use Only (FOUO)" if the "who" is removed, allowing more entities to take action to protect their networks and users based on this information.

Recommendation #3: Enhance Incident Response Capabilities

Problem: Arizona's cyber incident response capabilities need to be strengthened to stay ahead of evolving threats facing the state. Well-trained and agile cyber first responders are key to managing incidents and maintaining or regaining an effective continuum of operations by the affected entity.

Solution:
A. Strengthen Incident Response Capabilities statewide:

1. Provide collaborative teams to respond across the State to cyber incidents that have serious potential to impact the citizens and State of Arizona
2. Proactively set memorandums of understanding (MOUs) between state agencies and local governments to increase the effectiveness and timeliness of incident response
3. Invest in relationships within different sectors including to carry out incident response as smoothly as possible

B. Increase cyber incident management and response exercises across different sectors and localities statewide:

1. Anticipate incidents and allow the entities to practice skills of incident response before they occur
2. Expose local governments to the available resources and appropriate points of contact

Background: Incident response is critical to the security of Arizona during a cyber incident. This recommendation requires a relatively low fiscal impact for the coordination of the response teams and upkeep of the devices and systems used for incident response. Setting MOUs and maintaining relationships requires consistent communication between different localities, agencies, and private-sector partners but is achievable to pair with continuous exercises and meetings with these groups.

Recommendation #4: Enhance Cyberinfrastructure to Protect Consumers

Problem:
Arizona works to provide government services at the speed of business, meaning the government must adapt to technological changes while also keeping consumer information safe. Almost all new and emerging technologies involve the collection and use of vast amounts of consumer data. In turn, many state contractors who utilize such technologies may have access to highly sensitive and/or personal information relating to individual Arizona residents, local small businesses, or government operations. The ACT underscores state actions which will protect the infrastructure supporting the efficiency of government and the security of information required to provide Arizonans with services.

Solution:
A. Update state procurement rules:

1. Consider updating state procurement laws and regulations to include more stringent data privacy and cybersecurity requirements for vendors and partners gaining access to state systems
2. Prioritize cyber risk insurance when evaluating third-party contracts and vendors.

B. Invest in Cyber Risk Management Best Practices:

1. Consider funding cyber risk insurance for Arizona's government agencies across enterprise networks
2. Continue to fund statewide cybersecurity controls that align with the National Institute of Standards and Technology (NIST) cybersecurity standards to protect consumer data
3. Continue to share cybersecurity risk information between state agencies, different branches of government, and the private sector

Background: Codifying cybersecurity requirements into State procurement laws and investing in cyber risk management best practices should make the state's priorities and the contractors' obligations clear.

Meeting NIST cybersecurity standards is required to receive data that we transmit, process, and store from the federal government. This consumer data is necessary to provide critical government services. However, this citizen data is increasingly under attack from criminal hackers and, therefore, steps must be taken to further protect it.

Recommendation #5: Create a Unified State Brand - “CyberAZ”

Problem: Cybersecurity experts, educators, government officials, and private-sector leaders are continually asked why a “go-to” resource for cyber information and incident reporting does not exist. The information overload and perceived complexity of cybersecurity threats often overwhelms those who are unfamiliar with cybersecurity, resulting in a lack of consumer knowledge or trust in the resources available. The ACT has identified this lack of a single “go-to” resource as an opportunity for Arizona to drive change in cybersecurity and to be seen more widely as a leader in cybersecurity.

Solution:

A. Create a state-level website that is easy to find and contains relevant, basic security information with an Arizona-based context. The unified brand will serve in educating the following groups:

1. Arizona citizens, regarding how they can protect themselves;
2. Arizona citizens, regarding career opportunities in cybersecurity;
3. Arizona employers, regarding strategies for attracting, retaining, and developing cybersecurity talent; and
4. US employers and citizens, as well as bad actors, regarding Arizona's strong stance on cybersecurity.

B. Develop a supportive in-state and out-of-state marketing effort to broaden the reach of CyberAZ brand and make “cyber.az.gov” a go-to destination

C. Develop core talking points and a cybersecurity Speaker's Bureau (ambassadors/champions) to disseminate cyber safety information to the community

Background: Ideally an ever-expanding resource, this single “go-to” website would give the general population access to cyber safety information, career and education opportunities, and eventually allow Arizonans to report and learn about some of the most frequent cyber crimes impacting our state.

The State of Arizona can host the website. Branding and a strong web presence are critical components of a robust economic development strategy that highlights Arizona's healthy cyber ecosystem, supports new business attraction and existing business growth, and develops and attracts new talent to Arizona. Arizona Commerce Authority (ACA) is a strong partner that can be instrumental in branding efforts. Development of these messaging materials and collateral would have minor costs and effectively spread valuable information.

Recommendation #6: Create a "Call to Action" to Enhance Cyber Safety Education for K-12

Problem: Cyber safety is the responsibility of everyone with access to cyberspace. We know that 99% of all cyber incidents are the result of someone clicking a malicious link, meaning that much of the responsibility is on the cyber user to keep themselves and others cyber safe online. This is especially dangerous for children who are accessing the Internet at a younger age, before being exposed to optimal cyber safety practices from their parents or peers. Lack of knowledge about cybersecurity and proper cyber safety practices among children is one of the reasons that K-12 is among the least secure industry sectors.. The ACT sees this as a huge opportunity to thwart risk to Arizonans. The ACT recommends addressing this vulnerability head-on by meeting the cyber users where they are at, -- in the classrooms across Arizona -- and encouraging younger generations to practice cyber safety daily. Consequently, this training has an opportunity to create downstream learning opportunities for these students' teachers, families, and communities.

Solution:
A. Enhance and expand Cyber Safety education opportunities in all school districts through increased availability of resources, materials, and curriculum for all students

B. Create and implement a "Cyber Safe K-12" District and School award to recognize the implementation of high-quality cyber safety programs and competitions

Background: A comprehensive "Call to Action" increases the sense of urgency for K-12 cyber safety education and helps address the issues of human error and actions, which play a significant role in cyber incidents. The allocation of resources, incentives, rewards, and recognition demonstrates the State's prioritization of this goal. Moreover, the three-year timeline acknowledges school districts' need to develop capacity through training and professional development for effective implementation.

This recommendation may require funding to reach 600 districts and charters for a "train the trainer" model and materials, over a three year period. Improving awareness of cyber safe practices will reduce inadvertent unsecured practices by students, faculty, and staff, resulting in reduced cyber incidents and attacks at schools and homes. This investment will provide a significant return on investment and increase the cost to the hacker.

Recommendation #7: Extend Opportunities to Support the Cyber Talent Pipeline

Problem: Arizona has a shortage of teachers, faculty, and real-world learning opportunities needed to support cyber education for future workforce needs and economic development.

Solution:

A. Ensure Arizona has the teachers and faculty to teach cyber-related topics:

1. Create a Cybersecurity Educator program to attract, recruit, retain, and recognize high school and post-secondary cybersecurity educators
    - Strategies: company support for employees serving as "adjunct" faculty and teachers, scholarships, tuition assistance, and loan forgiveness for program completion and certification (e.g., dual-enrollment certifications)
2. Use the technology available for online and remote access to share teaching resources, and to increase access to high-quality cybersecurity instruction as outlined in Arizona's computer science education standards

B. Increase opportunities for cyber internships and externships within state government

1. Identify openings and opportunities in state government that could be filled by interns to gain real-world experience while finishing or continuing education
    - Strategies: increase the availability of industry internships/externships to reward, retain, and attract educators and students to Arizona
2. Use the technology available for online, remote access, and to share teaching resources, and disseminate opportunities to students in rural areas

C. Encourage continued private-sector engagement

1. Support industry sector partnerships to:
    - identify cyber workforce challenges, opportunities, and recommendations;
    - coordinate industry, education, and workforce partners;
    - leverage resources to increase the supply of talent in Arizona; and
    - Strategies: hiring from a broader range of degrees and supplementing with cybersecurity specific training and credentials, alternative talent strategies like boot camps and apprenticeships, and developing/upskilling current employees.
2. Support cross-sector engagement and relationships to provide opportunities and funding for strategies

Background: Arizona has an opportunity to invest in the talent pipeline from primary to post-secondary education and training. By utilizing existing infrastructure and top-notch instructors within the state, to reach schools and districts across the state while increasing future opportunities for teachers who may not yet feel comfortable teaching these topics in their classrooms.

The state also has an opportunity to lead by example, using and encouraging internships, externships, and MOUs to provide real-world experience to those learning cyber-related skills while receiving their insight and expertise in return.