COHESITY ATARC WHITE PAPER

The Constant Shifts in Attack Surface and the Impact on Cybersecurity

Summary of Roundtable, co-hosted by Cohesity and ATARC in December 2022

Attack Surface Defined

ANY exposure to a hostile entity:

- Internet gateways
- Third party code
- Data transition points
- All of the above and more

If you were to ask a handful of cybersecurity professionals for the definition of attack surface, you would likely receive a handful of different answers. While the definition of 'attack surface' may differ, the concept remains the same, that an attack surface is any exposure to a hostile entity.

From a network perspective, the exposure may be internet gateways. For software developers, exposure may be within the supply-chain where code is introduced by a third party. Data analysts might consider the attack surface as a data transition point from on-premise environment to the cloud backup. From a CISO's perspective, the attack surface is all of the above, and more.

The phrase 'reducing attack surface' is considered a key tenant in many cybersecurity philosophies. It's used frequently among cybersecurity professionals to describe reducing exposed threats. The question lies in whether 'reducing attack surface' actually reduces exposure to threats, or if the act just changes the vectors used by hostile actors to access critical data.

What started as a term referencing threats from internet exposure, attack surface has evolved to something more complex. In today's cyber-world, all potential ways to bypass traditional perimeter controls must be considered. By considering all aspects of exposure, attack surface shifts from a focus on architecture to threat capabilities.

In partnership with Cohesity, the Advanced Technology Academic Research Center (ATARC) recently hosted a roundtable of government experts to discuss how advanced technologies, hostile actor sophistication and social engineering has forced us to look at the term "attack surface" in a different light.

How to Define 'Attack Surface'?

One roundtable participant considers attack surface through two lenses: staff and devices. Agencies often manage hundreds, if not thousands of personnel, as well as their devices and applications. In a world connected to the internet, all devices with a

digital component and their users have the potential to be compromised and can be considered an attack surface.

Key Takeaway

We need to make sure we're questioning the convention of what we secure and how we secure it.

Whether attack surfaces increase, expand, change, or shift, the challenges of an evolving threat landscape remain consistent. With perimeterless networks and the expansion of the internet of things, visibility must be integrated into all aspects of an agency's cybersecurity stack. To manage the complexity of shifting attack surfaces, agencies at the roundtable shared they are working to prioritize visibility, primarily with Zero Trust principles like identity.

New technology capabilities enable agencies to integrate this level of security into all aspects of cybersecurity, but also things like workflows, machine learning models, and AI services. With access to vast amounts of data, agencies can now better detect anomalies and fix problems without human intervention.

While new technology is helping agencies to better manage shifts in attack surface, some roundtable participants caution that agencies must also have a bit of blind trust in the security of vendor solutions. Other participants share that because many agencies cannot simply patch systems and devices, the vendor community needs to work at the same pace as agencies to manage threats more effectively.

Challenges with Shifting Attack Surfaces

Managing attack surfaces in a perimeterless network environment and a constantly evolving remote workforce is one thing, but managing all devices connected to the internet is another. From electronic coffee mugs to sensors on bridges, a large majority of our everyday life is connected to the internet, and should be considered a part of the attack surface.

For many of these connected devices, it is likely that manufacturers were not thinking about security features during development. Rather, they were more focused on being first-to-market. Now, agencies must consider attack surface in terms of potential loss of life. A roundtable participant questions what happens if a safety feature on a bridge were to fail or predictive maintenance of a plane did not register?

With more devices being connected to the internet every day, government agencies inherently have less control over the attack surface. Similarly, as agencies transition to SaaS and Cloud-native solutions, they become more and more dependent on their vendors to supply robust security capabilities. Agencies must trust that the aggregate set of responsibilities between provider and customer allow agencies to conduct basic recovery response operations in worst case incident scenarios.

Without complete ownership or oversight of security stacks, agencies may need to get more creative with how they access data and information from vendor-controlled solutions. Without full access to data, agency is visibility weakened. While a greater reliance on Cloud and SaaS solutions brings challenges, some roundtable participants consider these shifts in attack surface as an opportunity to improve and reimagine operations.

A Reimagined Future

With shifts and expansions of attack surfaces across devices and Cloud networks, the reality is that anyone can be a target, whether an attacker targeted them or not. While there may be increased risk in Cloud operations, roundtable participants believe opportunity can be found. In this global IT environment, where the supply chain ecosystem connects everyone, agencies have a unique opportunity to reimagine how they approach both operations and cybersecurity.

Being cyber-resilient means more than implementing new technology. Participants share that everyone, including leadership and IT staff, should continue to upskill themselves in this new and evolving threat environment in order to keep pace. Ensuring staff understand the vision of leadership and an understanding of what tomorrow could look like is important for an agency to develop cyber resilience.

Education and upskilling all employees is especially critical for small organizations that have few resources earmarked for cybersecurity. As more Federal workers retire, agencies will need to train existing staff and bring in new talent with a focus on developing a strong culture around cybersecurity. Since the attack surface will continue to shift and expand, agencies will also need to proactively consider the skills teams will need six months from now. Continuous training and upskilling will help develop a culture adept in cybersecurity and willing to report suspicious activity.

Learn more about how Cohesity can help protect agency data, as well as its data management and back-up solutions.

Get involved in ATARC Working Groups and other ATARC Events!