Cyber Committee

Security and Cloud Computing

Security remains the number one obstacle to adoption of cloud computing for businesses and federal agencies. Public cloud solutions are seen as the most vulnerable options from a security perspective, leaving many federal customers to seek private alternatives to overcome security challenges. Regardless of the deployment model selected--private, public, community, or hybrid—conquering security concerns is required for cloud computing to achieve its full potential as the next generation of IT architecture. Recent trends in cloud computing demonstrate the architecture has matured and offers distinct advantages for cyber security defense. Lessons learned continue to emerge with three areas of focus described here: visibility, collaboration, and workforce enrichment.

This document is a collective representation of senior cyber leadership views from more than two dozen private, federal, academic, and other institutions associated with the AFCEA Cyber Committee.

***Visibility*: Cloud computing offers significantly improved visibility and insight that is driving new cyber security solutions.**

Access to cloud computing services in traditional classified environments and in modern mobile environments provides numerous opportunities to gain visibility and retrieve security data points across your infrastructure, platforms, and applications. Collecting pulse points from the high-speed networks used to connect to your cloud provides insight into threats attempting to breach the perimeter of your infrastructure. Remote access devices and global position/location can be detected through other data points, triggering the requirement for additional security access and authorization controls while also providing real-time knowledge of the security status of end-user devices. Constant monitoring of applications and platforms offers additional data collection points for discovering vulnerabilities in applications that can be used to infiltrate the infrastructure. Moreover, merging measures and metrics from co-located environments or other cloud locations in your global enterprise can add yet another layer of data to the collection.

Establishing robust administrative and network management consoles designed to collate these numerous measures and metrics result in a level of security insight not previously achieved prior to cloud computing. Data points from routers, switches, firewalls, load balancers, storage networks, applications, and end-user devices combined with satellite, terrestrial, and wireless access methods allow true end-to-end security knowledge to identify, isolate, and eradicate breaches while minimizing impact and preserving mission.

New cyber security and IT service management products are emerging to provide real-time, deep insight of metrics collected in the cloud computing infrastructure. Visibility provided through new exploitation and analysis products will significantly enhance prevention of and rapid response to cyber intrusions.

Utilities to migrate applications into the cloud provide other forms of visibility for security and application baseline management. Best practices for migration recommend a complete application inventory and analysis. The visibility derived from this inventory can be used to streamline legacy applications, accelerate implementation of common services, and confirm your organization's compliance with various continuity, disaster recovery, or legal reporting requirements. Structured virtualization migration processes contain code baseline inspections which can be used to identify assurance vulnerabilities in legacy applications. Overall, using a disciplined approach when implementing cloud computing optimizes your application baseline and improves your overall security posture.

Additional benefits derived from the cloud's ability to support robust collection of metrics is the parsing and analyzing of such data for other purposes. For example, individual usage patterns can be analyzed to a finer level of detail to support a variety of business purposes including enhanced customer experience and counterintelligence audit. Access to more granular performance data from all of the devices connected to your cloud allows deep analytics for load balancing refinement to support decisions on where and how to cache data for best end-user support. You can drive more efficient usage of cloud resources with better understanding of available capacity based on real-time performance data. Finally, as a customer of cloud, the robust collection of metrics can provide dashboard views of your specific resource consumption thus allowing you to pay for only what you use with confidence.

***Collaboration*: Cloud computing facilitates new government-industry partnerships for enhanced protection of national interests.**

Knowledge gained through improved visibility can be rapidly shared between government and industry to further widen the blanket of security protection. Quick identification of potential breaches by either government or industry allows faster communication and broader dissemination of detailed information on exploitation, attack, or exfiltration attempts. Widespread information sharing will appreciably improve the speed and depth of defensive response to enable broad spectrum protection of classified and unclassified information. Current computing architectures can limit visibility and sharing between government and industry--resulting in delayed reactions to breaches.

In the unfortunate event a serious cyber security incident occurs for government or industry, the vast collection of data from the cloud can be used for government-industry investigation. Inspecting massive amounts of information—stored and readily available—can accelerate understanding of an event, its consequences, and proper response. Government-industry partnerships also encourage comparison and validation of operating assumptions related to cyber security breach attempts and intrusions, thus enhancing progress on advanced defensive implementations.

The advantages of public-private partnerships extend beyond the improved visibility provided. Collaboration between government and industry means greater influence on regulatory and compliance requirements--the overwhelming majority of which were established in a non-cloud computing world. Working together, public and private organizations can drive policies in directions that promote future mission/business needs while also safeguarding our infrastructures and information. In addition, the partnerships can identify technical limitations in current cloud computing capabilities—whether security, performance, or utility—and drive improvements in products and architectures to overcome limitations. As an example, new non-hypervisor based clouds are emerging in response to partnership pressures for better performance with "big data", computationally-intensive, and high-volume data collections that have not responded well to performance impacts created in the hypervisor layer.

Workforce Enrichment**: Cloud computing is spotlighting the need for a new generation of IT professionals that are a blend of IT and security.**

Training tomorrow's IT workforce to rapidly identify and respond to cyber events requires new forms of traditional information security (IS) classroom training and innovative forms of on-the-job training. Cloud computing has highlighted weaknesses in traditional security training for our IT workforce. The plethora of data available through the many sensors described above can produce an overwhelming landscape of information that must be quickly analyzed and isolated to produce real-time defensive responses for IT teams. Merging the IS and IT disciplines, combined with the development and implementation of formal and informal training programs to quickly increase the IS skill set of IT professionals, is absolutely necessary for the future.

Academic programs should be shaped to create this blended workforce. Organizations will need to bridge the gap while universities produce the workforce with needed competencies. The bridge can be built initially by training the IT workforce on how to collate, assess, analyze, and respond to the insights generated through the cloud's many points of visibility. Use case scenarios based on real or fabricated intrusions can serve as excellent teaching tools and offer the added benefit of linking IT experts with junior IT professionals in a mentor program that can produce additional returns on the training investment.

IT administrators spend too much of their time performing security patch and maintenance operations, which detracts from time available for higher value contributions to the IT enterprise and for learning new tools/techniques. Cloud computing offers improved security by reducing requirements for global deployment of "fat" or "thick" client devices, which can be dangerous infiltration points and require constant patch management. Hard drives aren't necessary for access to cloud computing services, when such services are architected and implemented properly. End users can gain access to all information, applications, and services through thin client PCs, virtual desktop implementations, and wireless devices. This has an added benefit of improving corporate information security through rapid, near real-time deployment of security patches/upgrades. Moreover, the rapid deployment of patches gives administrators more time to learn new methodologies, perform deeper analysis of security events, and implement new processes to prevent future intrusions.

***Summary*:** Security obstacles surrounding cloud computing are being proactively addressed in a number of ways. Industry is creating partnerships to drive cloud computing standards and increase interoperability. Cloud computing alliances are forming to introduce innovative technologies designed to capitalize on the insights provided through cloud computing and produce enhanced cyber security awareness at all layers of the IT stack. Combining interoperability standards with improved cyber tools will give the IT workforce the capabilities needed to safeguard information and add value to mission.