SECURITYIN30
LIVE WITH ALLEGION

Part One: Growing Acceptance of Cloud-based Access Control

October 15, 2021

Question & Answer

Q. Have you had success using funds for deploying solutions, ESSER, etc.?

A. ICOE is exploring ESSR funds as part of our COVID Contact Tracing efforts leveraging general fund dollars geared toward facilities and safety measures. California Office of Emergency Services (CALOES) occasionally offers grants for safety initiative such as video surveillance.

Q. How can folks leverage existing support locally or industry organizations

A. Most state have organizations for School Resources Officers, IT professionals, etc., that have periodic meetings and industry trade shows. These are a great source of information and opportunity to build local relationships for best practice sharing. For example, California IT in Education (CITE) – www.cite.org. This association offers district technology leaders to share experiences in implementation of systems and provides networking opportunities with companies in this industry at their annual conference.

Q. Was moving to the cloud part of a movement of much of technology stack and access control became part of that transition? Or did it lead the move to the cloud?

A. While security is one of the first systems ICOE moved to the cloud, ICOE has transitioned several other systems to the cloud. We started with our e-mail/collaboration platform Microsoft Exchange to Exchange Online. Our most recent migration has been our voice communication from Cisco VoIP on-premises platform to Microsoft Teams. Other systems we've migrated to the cloud are Domain Name Services (DNS), cold storage backups, Absence Management System (Frontline), Help Desk Software (Freshworks) etc.

Q. Are there lessons learned you could share based on your transition to cloud-based?

A.

- Ensure full integration of physical lock features with cloud control systems
- Understand Power Over Ethernet (PoE) requirements and appropriately size power and battery systems to match your service levels.
- Ensure adequate network capacity between your infrastructure and the cloud infrastructure.
- Ensure installers are certified on both the physical infrastructure and cloud management platforms.
- Synergize access control with surveillance by adding camera(s) at each access-controlled door where possible.
- When designing new buildings, ensure doors are wired for access control to minimize future costs of retrofitting doors. Also, include network connections on possible video camera locations.

Q. Can you speak towards ROI and the reoccurring fees of cloud-based systems?

A.

- Costs of hardware and licensing are known upfront. And your TCO/ROI costs are easier to calculate. The cloud infrastructure transfers many of the management components needed to operate the system (servers, storage, security) to cloud infrastructure, which is elastic and transparent to the customer.
- Reduces shadow costs, usually in the form of staff resources spending time maintain the system, data center costs to operate servers (power, cooling, patching, upgrades, etc.)
- Fees will vary between cloud providers. Investigate if the provider offers pricing structures for your industry such as government or educational institution pricing.

Q. What is the probability that a cloud-based system could be hacked, and all data could be compromised?

A. Like any system, a cloud-based system can be hacked. So, it is important take time to understand the security practices from your cloud provider and ensure best practices are followed. to ensure your service provider has the appropriate security measures in place to deter potential hacks like file encryption, strong firewalls, data backups and policies around managing security updates. Additional measures to help prevent hacks such as safeguarding against credential theft, requiring multi-factor authentication and prohibit credential sharing are also extremely important to securing your data. Single Sign-on (through your cloud directory services), Role-based access, minimizing administrative privileges and provide role-based technical support are important mechanisms to mitigate risks.

Q. How do you conduct a vulnerability test with your access control?

A. At ICOE, we conduct monthly vulnerability scanning against all public facing systems (meaning they have open ports exposed on the firewall). These reports help us mitigate any potential software bugs and known vulnerabilities and allow us to make configuration corrections or apply software updates on a timely manner. The vulnerability database is updated on weekly bases. As an added safety precaution, the access control panels are not accessible from the Internet and secured behind our firewall.