Webinar Summary

Doing More With Less:

A Smarter Approach to Bank Physical Security Operations

Webinar Hosted June 24, 2026 by: Nikki Williams, North American Regional Marketing Manager at ICT

Panelists: Kent Howell, Director of Business Development, DAC | John Valadez, Senior Account Executive, Central Texas, DAC | Travis Chaffin, Regional Sales Manager, Central & North Texas, ICT | Alex Sawhney, Regional Sales Manager, South Texas, ICT

Banking security leaders are being asked to protect more branches, manage greater risk, and support evolving business operations, all while working with leaner teams and tighter budgets. In ICT and DAC's ***Doing More with Less: A Smarter Approach to Bank Physical Security Operations*** webinar discussion, banking security experts shared practical strategies, real-world lessons, and key questions every financial institution should be asking. The most valuable takeaways are summarized below.

Fragmentation Is the Root Problem

Banks that have grown through acquisitions often inherit a patchwork of disconnected security systems — each with different interfaces, different capabilities, and different management demands. The result: security teams spend more time managing tools than managing security.

> *"The biggest issue is fragmentation, having too many systems. Each one is different to use, different to manage, and may or may not have the same features."*
> Travis Chaffin, Regional Sales Manager, Central & North Texas, ICT

> *"When systems don't talk to each other, the backend troubleshooting aspect is a big time waster."*
> Kent Howell, Director of Business Development, DAC

Standardization Is the Solution

The antidote to fragmentation isn't just better technology, it's standardizing on a single platform across all locations. Standardization reduces training burden, speeds up onboarding, simplifies compliance reporting, and makes multi-branch management genuinely scalable.

> *"How do you achieve doing more with less? How do you become compliant? How do you bring branches on quicker? It's really about standardizing the product you're using."*
> Kent Howell, Director of Business Development, DAC

Multi-Branch Visibility Changes Everything

For banks managing dozens or hundreds of branches across wide geographies, the ability to monitor, manage, and respond remotely is no longer a nice-to-have, it's a necessity. Panelists shared real-world examples of IT teams that once drove hours to troubleshoot individual branches, and now rarely leave headquarters.

> *"Having that central visibility, that central location where you can handle basic functionality, is a huge aspect. You need immediate eyes on it if something isn't functioning properly."*
> Alex Sawhney, Regional Sales Manager, South Texas, ICT

> *"About a year after completing the project, their IT team told me: "We never have to go to a branch anymore." They just stay in headquarters. That's a good problem to have."*
> Kent Howell, Director of Business Development, DAC

The Hidden Cost of Siloed Systems

Separate, disconnected systems don't just create operational friction, they create financial exposure. Without a unified view, banks lose visibility into equipment health, lifecycle planning, and budget forecasting. Unified platforms make those costs predictable.

> *"A unified platform can tell you when your cameras or card readers are approaching end of life, so you can plan for it, budget for it, instead of scrambling when something goes down."*
> John Valadez, Senior Account Executive – Central Texas, DAC

Ask the Weird Questions

One of the most memorable pieces of advice from the panel: don't limit your discovery conversations to standard security terminology. Describe desired outcomes, and go big in your requests. The best installations come from clients who said "when I hit this button, I want this to happen", then let the integrator figure it out and advise you on all the possibilities and custom solutions.

> *"A lot of times, things get lost when we're too rigid with vocabulary. Tell us what you want to happen. Then let the professionals make it work."*
> Travis Chaffin, Regional Sales Manager, Central & North Texas, ICT

> *"Ask the weird questions. Ask about scenarios you want to plan for. If you don't ask, we might not know that something is important to you and your system needs."*
> Alex Sawhney, Regional Sales Manager, South Texas, ICT

Questions Every Bank Security Leader Should Ask

The webinar ended with some suggested questions all make security decision makers should ask their security integrators.

Is our current system still supported?
End-of-life hardware creates emergency replacements. Build system lifecycle reviews into your annual security audit.

Can we absorb 5 new branches tomorrow?

If your answer is uncertain, your platform isn't built for growth. Scalability should be a requirement, not an afterthought.

Who else needs a seat at the table?
Security decisions touch IT (cybersecurity, network hardening), HR (credential provisioning), and operations. Involve them early.

What happens when something goes down?
Ask your security integrator what the response time is. Are remote diagnostics available? What's the plan if a branch goes offline?

Are we including security in our AI conversation?
AI is already changing physical security, from intelligent video monitoring to predictive alerts. Ask vendors how they're investing in it now and make sure AI in security is part of budgeting conversations.

Overall Takeaway

Banks that standardize on a unified platform aren't just improving security, they're reclaiming time, reducing cost, and building an infrastructure ready for whatever growth comes next. The right security integrator doesn't just install a system. They help you think through every scenario, ask the questions you haven't thought of yet, and build something that grows with you.

Watch the Complete Webinar Online HERE.