Best Practices for Multi-Site Security Management

Companies operating at a single site or at regional sites, but looking to expand nationwide or even internationally, will face a number of challenges as they move away from their existing infrastructure, select a new security system, and seek to implement that system cost effectively and successfully. A recent webinar hosted by ASIS International and Brivo discussed the challenges of multi-site security management and how cloud-based systems can help companies run their security programs more efficiently as they grow, allowing them to support the business mission and reduce costs.

One company that made the change to a multi-site security system is Plains Capital Bank, which turned to a cloud-based security solution

> **"The systems were functioning – in the user experience the doors would unlock – but it was really on the back end where we had some struggles. We wanted to pull that together and get that into a language that would resonate with our leadership."**
>
> **Bill Lines, Chief Information Security Officer at Plains Capital Bank**

provided by Brivo. Bill Lines, Chief Information Security Officer at Plains Capital Bank, said that as the company grew the staff discovered that they were managing multiple existing systems with varying levels of technology. Users were carrying multiple credentials, creating a disjointed user experience and operational inefficiencies.

The company's security team wanted to have a single secure system with a single secure credential to meet its current needs and those into the future. "We decided the system should focus on ensuring data integrity across the life cycle of the product, as well as data disaster recovery and system resiliency," Lines said. "It also needed to be highly skillable and light on IT resources, without impacting any of the other enterprise projects happening within the IT organization or within bank operations."

In creating their master plan, Lines said they had to answer the question, "If it isn't broken, why fix it? The systems were functioning – in the user experience the doors would unlock – but it was really on the back end where we had some struggles. We wanted to pull that together and get that into a language that would resonate with our leadership," Lines said.

"A well-crafted multi-site program can support a business' growth and help it run more efficiently," said John Szczygiel, Chief Operating Officer at Brivo. It can enable the workforce, provide better protection for assets and information, and reduce the time to complete audits and inspections. Such a program can be critical as more people work from multiple locations.

Szczygiel cited one example of a client whose consultants, when traveling to remote locations, would often take hours to get in the building, get themselves credentialed, and set up at a work space. "These were well-compensated consultants who had high billable rates, so that was costing the company a lot of money," Szczygiel said. A simple integration with a hoteling system allowed the consultants to pre-register to use a particular facility, so they were able to get in the door with their credentials, find their work station and needed resources, and get to work quickly. "So we cut down from about one to two hours to get a workspace set up to just a few minutes," Szczygiel said. "That's one example of how a multi-site program with some thoughtful integrations can help impact the business."

In addition to enabling the workforce, a consistent multi-site program also enables better protection for assets and information while reducing costs. It can facilitate the audit and inspection routines that are part of most businesses, reduce the risk of non-compliance, and enable integration with enterprise systems to share data and reduce re-work.

Lines said by using cloud technology and relying on experts to handle the back-end infrastructure, his company was able to improve the security program and focus on the business of securing the bank, as well as save costs. "By implementing multi-technology mobile-enabled readers, integrating our new credentials with some of our base buildings, conducting a mobile credential rollout, and allowing some flexibility with our credentials, we were able to demonstrate an improved security experience while reducing some operational cost," Lines said.

Understanding Challenges of Multi-Site Security

Setting up a multi-site security program comes with challenges, from gaining organizational buy-in to developing a strong return on investment and overcoming budget limitations. Szczygiel said it's important to balance practical considerations, such as budget, time, culture, and even construction process, with the security objectives. "One way to achieve a good security program is to align what you're doing with the business objective, so people see security as supporting and furthering what they're trying to get done with the business," he said.

Lines agreed. "For us, aligning the security initiatives with business strategies and objectives turned the conversation into a different type of discussion. If you understand the strategic plan of the business, you can put your objectives into meaningful concepts that our executives can take away, and then that segues into conversations around budgeting."

When implementing a multi-site security program, companies should consider how the processes and systems they select for an individual site will work at multiple sites. Szczygiel said companies should avoid thinking locally to make good long term choices. "There are simple solutions that work well and are cost effective, but they don't really scale," he said. "So you need to consider how this system will grow and how it will be supported as it gets multiplied in multiple locations."

Any new system also should meet IT standards. The system will operate on the company network, so the status of the devices and how well they comply with IT regulations and policies will be important. "They may be less visible at the local level, but as you move up the continuum

to the national and global levels, they become more important," Szczygiel said.

For example, because Plains Capital Bank is a Texas-chartered financial institution but also part of a publicly traded financial services holding company, the security program had to encompass the broader organization. "We wanted to make sure whatever decision we made locally would also translate to an enterprise level, not just thinking about the bank but also thinking about our sister companies as well," Lines said. "We wanted to focus on security services and not system functionality, so things like break fix, annual maintenance, automated services call out, not having to worry about software, hardware, client configuration, was important to our program as we scaled from local to beyond."

With a sound foundation of decisions at the local level, companies should be in good position for a country-wide expansion. "The key here are making sure that the installation and support network that you've chosen is extensible," Szczygiel said. "You need to make sure the technology you select on the local level can operate on your company's wide-area network or on the internet." Brivo, for example, operates on common broadband connections, so whether companies have simple internet or cellular services, they can get these systems up and running quickly.

Going to multiple geographically dispersed sites means a number of local personnel interacting with the system. Previously, that most likely would have involved a fixed client installation and the involvement of IT. "But having a browser, a mobile-only solution, is going to save you a lot of time and money, because you're not going to need PC upgrades that you might discover as you go through these sites and realize that you don't have the hardware to run your software on," Szczygiel said . With a browser-based system like Brivo, those problems can be handled simply.

Also, any program that expands to multiple sites should enable companies to cut down on duplicate work, like entering employee names and credentials. "With one nationwide system that's much simpler, because one employee record can be shared with multiple sites without duplicating it," Szczygiel said. "Also, you can make that even more simple by leveraging an integration with your IT infrastructure, something like directory that would allow you to add, delete, or suspend employees automatically, rather than security folks having to go in and hand make changes for every employee."

An organization that is expanding internationally can face even more challenges, including time zone issues, logistical issues about getting products into certain countries, language barriers, legal norms, and cultural differences. Szczygiel cited one example of a customer operating in a different culture that doesn't see anything wrong with sharing badges. "So they were running into some problems when they realized that employees would simply hand other employees their badge. There are also legal issues – different countries consider privacy differently. So things you can do in the Untied Stated may not be as acceptable in a country like France, for example." Any global implementation will most likely take more time, and companies should account for that in their scheduling and make sure their budgets can accommodate some of the ways work is done in other countries.

Facets of a Robust Program

A robust multi-site security program should contain four key facets, Szczygiel said, including documented standards, consistent implementation, infrastructure leverage, and a living plan.

Lines agreed that documenting standards is a core value in any security plan. "Developing strong physical security standards is key," he said.

"Those that describe an acceptable approach or a minimum approach no matter where the facility is located is what we strove for." He recommended that companies also make sure they get buy-in from their executives, stakeholders, and peers.

When establishing standards, companies should establish a facility protection standard, based on the risks and types of facilities that they have, Sczcygiel said. They also should establish equipment and vendor standards, because many companies run into trouble by using multiple types of technologies. For example, if companies choose a one-card solution, they need to make sure one card can work at all locations. Companies should also determine what program choices are made centrally versus regionally. "Many times regional offices have their own opinions, local customs, and preferences, so it's helpful upfront to know which things are optional, which things regional offices can choose, and which things are dictated," Sczcygiel said.

Having documented standards enables companies to have more consistency in their implementation. To achieve consistent implementation, companies must understand the costs involved. "If you don't have a clear sense of the scope of the work upfront, if you don't have a good way to control costs, it's going to be very difficult to communicate your budget needs," Sczcygiel said. "It's important to follow your documentation, understand the costs involved, and make sure you have ways to control them." He added that a cloud-based system is easier to budget for than something that's installed locally, which would involve computer infrastructure, networking costs, and other unknowns.

Sczcygiel also urged companies to get a seat at the construction table with IT and local management. "There are a lot decisions that need to be made at the architectural level that are going to impact your security budget, perhaps even your ability to secure certain types of doors or protect your facility, as well as the cost of the system," he said. "Also, picking products and vendors with proven extensibility isn't always easy but it is key. You need to make sure your products and vendors have a plan to be around for a long time, and as you grow and your needs change, they have the ability to grow with you."

By using cloud technology and relying on experts to handle the back-end infrastructure, his company was able to improve the security program and focus on the business of securing the bank

Bill Lines, Chief Information Security Officer at Plains Capital Bank

Also, companies should leverage any assets they already have with more modern systems in order to increase the value and impact of their programs. To do that, they must understand IT's processes and concerns. "Too often in physical security we avoid talking to IT," Sczcygiel said. "It's the opposite. We should see them as partners and talk to them routinely because they have an important mission just like physical security does, and collaborating with them and other

Facets of a robust program

Documented Standards

Establish facility security standards that can be applied globally

A Living Plan

Constantly monitor and adjust your standards and plans and business needs as threats evolve

Consistent Implementation

Make system and support choices that enable flexible implementation of the standards and avoid wide variations

Infrastructure Leverage

Work with company assets such as IT and business systems to increase the value and impact of your security program

stakeholders on a mutually agreeable plan is the way to move forward." Those conversations will help companies uncover efficiencies and additional values that can be achieved by sharing data with other business systems.

Lines recommended not to have a throw-away mentality when reviewing existing conditions or performing a gap analysis. "There may be some positive existing security components that could be leveraged into your new plan," he said. "So a rip-and-replace methodology doesn't always work, especially when there is a business in operation and certainly when you have budget considerations and constraints. Leveraging some of the existing previous investments into your new plan can ultimately benefit your program."

Companies should be willing and able to adjust their programs as needed. "As we work in the modern world, opportunities and threats change constantly, minute by minute," Sczcygiel said. "So it's important to know that your plan is going to evolve – it has to evolve in order to stay strong."

To achieve a living plan, companies should establish key success factors, closely monitor those success factors, and share them freely. "You want to avoid entropy or even failure in your program by aligning your key stakeholders to a few 'north stars' – those items that are recognized as a business value," Sczcygiel said. "Also, make sure your technology can evolve organically and rapidly, which are two different things. Sometimes they can evolve but not rapidly and not cost effectively."

Companies also should minimize any transition challenges that come with adding new software. "In the Brivo example, all of the software is hosted in the cloud so every one of our

customers is always on the same version of software, which is really difficult to say for any locally implemented system," Sczcygiel said. "So if we discover some new security vulnerability or threat or issue, we can deal with that quickly because we have one living organism of a system that is able to be updated on the fly."

At Plains Capital Bank, Lines said their "north star" was to take a cloud-first mentality with their program. "We were really keen on the reduction of infrastructure costs, pay as you go, and pay as you scale. Scalability for us was key," Lines said. "We wanted a mobile-enabled solution, we wanted a common credential, and we wanted to have that solution run securely across the network. We looked at it as more of just hardware and software but as a business enabler for the bank." In running the program, they focused on the amount of resources and how any new solution – either positive or negative – would impact staff hours. They also looked at the system performance and how that performance related to service-level agreements. Finally, they considered ease of installation and agile deployment in a standardized package.

Finally, if companies are not automating their physical security, then they will find it difficult to demonstrate compliance with various audits and regulatory standards. "This is where a well-crafted, multi-site security program really pays huge dividends," Sczcygiel said. "While it's not a big issue to collect real time data from one site, imagine doing that same audit if you have tens of or hundreds of disconnected sites. A single cloud-connected security platform is incredibly helpful here."

Achieving Results

In conclusion, when setting up a multi-site security program, it's important to establish standards that are applicable globally, whether that involves networking, hardware, or support mechanisms. Companies should develop strong value propositions that can be delivered by their security programs. And finally, they should select partners who can grow and evolve with them.

Companies should use cloud-based technology and make sure their solutions are cyber savvy. Any program should be able to be updated quickly, because new threats do emerge, and if companies are unable to push out a patch or make a change, they will not be agile enough in today's world to remain secure. Companies should make sure their programs are mobile and browser accessible, and they should avoid the challenges involved in having fixed client PC based systems. Also, any use of technology should be continually evolving.

"Focus your spending on the results you're trying to achieve, not the infrastructure that you think you need to build or a vendor would like to sell you," Szczygiel said. "You should be investing in services and not servers and software."