Strategic Risk Management

Protecting the business is a top priority for Banjercito

The threat landscape was changing and the mission of protecting a nationally critical bank demanded a dedicated security group and a strategic leader who possessed the passion and knowledge to build the new group from the ground up. This was the situation which Banco Nacional del Ejército, Fuerza Aérea y Armada (Banjercito) found itself in 2002. Responsible for banking services provided to the Mexican Army, Navy, and Air Force, along with managing the temporary import and entry of vehicles, Banjercito has a serious charge, one that warrants careful consideration when security and compliance are concerned.

Banjercito’s board of directors and CEO, General Fernando Millán Villegas, didn’t need to look very far to find someone to lead the newly formed security group. Tadeo Gutiérrez, who joined Banjercito in 1995 as a strategic planning and marketing manager, had demonstrated that he possessed an in-depth understanding of the bank’s business and an inclination to leverage technology solutions to solve new business requirements. For example, back in the late 1990s he contributed to an initiative to build out the bank’s first Internet presence.

Reporting directly to the CEO, Gutiérrez, the company’s chief information security and technology officer, is responsible for developing and maintaining Banjercito’s technology risk management strategy; the IT organization, a peer group to the Gutiérrez’ security group, is charged with implementation and day-to-day operations. “Security is always in the foreground for Banjercito,” Gutiérrez says. “Managing risk and protecting the business are top priorities for the organization.”

Upon assuming charge, the first thing Gutiérrez did was to propose an initiative to identify security and compliance gaps. In addition to new security challenges, the bank was in the process of rolling out Internet banking services. The Mexican National Bank Commission had also instituted certain regulations to which the bank needed to adhere. “We spent several years addressing those requirements and getting the right technologies in place,” Gutiérrez explains. “But it was more than just a technology play; we sought to address the organization’s culture—working to make security top of mind for all employees.”

Endpoint security: not like it used to be

Banjercito’s relationship with Symantec dates back to the 1990s when it began using Symantec firewalls and antivirus software. With the release of Symantec Endpoint Protection, the bank chose to upgrade in 2009.

Banjercito was able to consolidate the different endpoint security pieces down to one solution. “We have much broader coverage with Endpoint Protection—from antivirus and anti-spyware to intrusion detection and prevention and firewall,” Gutiérrez notes. “With everything in one centralized console, including reporting capabilities, we were able to reduce our capital expenditures while improving our IT staff productivity.”
Earlier this summer, Banjercito elected to upgrade to Symantec Endpoint Protection 12. “It improves how each device is identified,” Gutiérrez says. “And we’ve gotten more efficient managing our devices through the SONAR settings, whereby we can adjust scan settings to reduce false positive detection and other security-related issues.”

There’s an additional gain because of virtualization. Banjercito’s data center environment follows a strategic view to be highly virtualized, using VMware for Windows and Oracle VM Server for x86 Windows and UNIX. In those environments, Banjercito is seeing improved scan performance as a result of whitelisting files from the standard virtual machine image and optimizing scanning speeds and updates. Since many of the bank’s servers have high utilization rates, any degradation in performance could potentially impact the business.

Gutiérrez’ team is looking at other ways to protect Banjercito’s endpoints in the data center. They are currently in the process of testing Symantec Critical System Protection on select systems in the data center. “With Critical System Protection, we will have tighter integration with our VMware vSphere installation and the ability to write more granular policies to the level of each hypervisor,” Gutiérrez says.

Also part of the company’s larger endpoint security effort, Gutiérrez and his team proposed to rearchitect the company’s messaging security for the bank’s email systems in 2008. They elected to deploy two different solutions—one for external email and one for internal email. For internal email, they chose Symantec Messaging Gateway. It helped Banjercito slash the amount of internal spam and

“Managing risk and protecting the business are top priorities for the organization.”

– Tadeo Gutiérrez, Chief Information Security and Technology Officer, Banjercito

BANCO NACIONAL DEL EJÉRCITO, FUERZA AÉREA Y ARMADA

Founded: 1947
Employees: 1,485
Services: Credit and banking services for the Mexican armed forces personnel and diverse services for civilian and public dependencies

Tadeo Gutiérrez, Chief Information Security and Technology Officer, Banjercito
reduced its email infrastructure costs by allowing the bank to optimize the performance of its systems.

Security correlation for intelligent decision making

When Gutiérrez assumed charge of the security group in 2002, one of the top issues that he wanted to tackle was the correlation of security information across Banjercito’s IT environment. “It was an almost overwhelming task at the time, and our environment was less complex and much smaller than what it is today,” he recalls. “We had to expend a huge amount of time to capture a segment of the information that we get today.”

After evaluating several different solutions, the Banjercito team settled on Symantec Security Information Manager. “We were one of the first institutions in Mexico to begin using Symantec Security Information Manager,” Gutiérrez notes. “It has become a critical part of our larger risk management strategy. Our Security Operations Center runs daily reports using Security Information Manager to identify potential security issues and remediate where appropriate.”

The Security Operations Center also uses Security Information Manager to connect data from various proprietary data loss prevention tools, enabling a comprehensive view across Banjercito’s computing environments.

The need for an automated security management toolset that would support Banjercito’s heterogeneous computing environment—from the data center to the desktop—was an important criterion when Banjercito evaluated different solution options in 2002. “This was one of the reasons Security Information Manager was chosen,” Gutiérrez says. “It has proven the test of time and is a critical part of our risk management approach. We’re also able to fine tune baseline configuration policies and improve communications performance with the data we gather using Security Information Manager.”

In addition to improved risk posture, Banjercito has realized tangible productivity gains with Security Information Manager. Before its deployment, the bank had eight IT staff correlating security data. With Security Information Manager, Banjercito reduced this to four, reallocating the remaining staff to other business-critical initiatives.

### CRITICAL PIECES IN THE DATA CENTER

**Banjercito’s relationship**

with Symantec in the data center goes back to the late 1990s, when the bank first deployed Symantec NetBackup for backup and recovery. And while not part of Tadeo Gutiérrez’ responsibility, as they are part of the traditional IT function, he was able to comment on their role and function for this interview.

“Our first NetBackup implementation occurred before the formation of the security group,” Gutiérrez says. “And as our business grew and business requirements changed, NetBackup evolved along with them.”

For high availability on business-critical UNIX and Windows servers, Banjercito has relied upon Veritas Cluster Server for the past decade. The benefits extend beyond high availability. The multi-domain clustering capability reduces the bank’s hardware and software costs while giving it the ability to take systems offline for planned downtime without affecting availability. In 2008, Banjercito added Veritas Cluster File System to minimize system downtime even further. Cluster File System is used to create storage pools that are shared by multiple servers, enabling the Banjercito team to cut the time to provide data access during a time of failover.

In the early 2000s, “It was initially on business-critical servers,” Gutiérrez says. “Storage Foundation was then extended beyond just Oracle RAC installs to business-critical UNIX systems.” The IT team also uses Veritas Dynamic Multi-Pathing on many of those same systems. They are pleased with the results. For example, Banjercito has seen its utilization rates increase and remain at higher levels, an outcome that ultimately reduces its storage costs.

**“As our business grew and business requirements changed, NetBackup evolved along with them.”**

– Tadeo Gutiérrez, Chief Information Security and Technology Officer, Banjercito

The early 2000s. “It was initially on business-critical servers,” Gutiérrez says. “Storage Foundation was then extended beyond just Oracle RAC installs to business-critical UNIX systems.” The IT team also uses Veritas Dynamic Multi-Pathing on many of those same systems. They are pleased with the results. For example, Banjercito has seen its utilization rates increase and remain at higher levels, an outcome that ultimately reduces its storage costs.
Architecting messaging security

Shortly after implementing the new Symantec Messaging Gateway solution in 2008, as a result of an evolving threat landscape and emergence of new security standards, the Security team went in search of a compliance toolset. The Mexican government was preparing to pass new security standards designated as the General Management Administration for Technology and Communications and Security. It aggregates policies and benchmarks from various security standards such as ISO27001.

Banjercito was ahead of the game

Banjercito was ahead of the game when the new standards were issued by the Mexican government. With the formation of the security group, Gutiérrez and his team had adopted several security standards, including ISO27001, PCI, and COBIT, among others. As the Security team began looking at different solution options, they wanted to find more than a reporting tool. They sought a solution that would further strengthen the bank’s risk management capabilities. “Symantec Control Compliance Suite fit our criteria,” Gutiérrez reports.

As part of the initial rollout of the solution, Gutiérrez’ team collaborated with various members from the business and the IT team to identify and develop policies that Control Compliance Suite would enforce, based on the Banjercito’s business requirements. “It was a much broader approach than simply IT security standards,” he observes. “In addition to the new requirements from the Mexican government, the business pinpointed various compliance requirements. By engaging them in the policy-definition phase, we not only ensured that we captured business risks but held the different business owners accountable for their different areas.”

Certain policies were addressed with predefined policies in Control Compliance Suite. This was the case with a large number of the policies that were identified. “We were able to address these with Control Compliance Suite Policy Manager,” Gutiérrez says. “But others, more specific to the business as well as those spelled out in the new compliance regulation from the government, required custom-built policies.”

When Banjercito upgraded to the latest release of Control Compliance Suite in 2012, the bank added Control Compliance Suite Risk Manager. “It fits very nicely into our larger risk management strategy,” Gutiérrez states. “Working with the business, we defined risk thresholds and report on them.” These are included in the daily reports the Security team produces with Security Information Manager. “The reports facilitate a risk management discussion,” Gutiérrez explains. For areas that exceed thresholds, we are able to work with them to remediate problems. It becomes a collaborative process.”

But the risk management program doesn’t stop there for Banjercito. The Security team provides the bank’s CEO with weekly risk management reports and bimonthly reports to the board of directors. “Risks change on a regular basis; hence the reason we deliver risk management reports at this level of frequency,” Gutiérrez says. “In addition, accountability with the business only occurs when you keep them informed about risks on a regular basis.”

Commissioning data loss prevention

In 2010, Banjercito determined to deploy a solution to address data
loss prevention requirements. “It was a gap that we knew existed,” Gutiérrez relates. “We had information on the network that we couldn’t monitor and manage.”

Banjercito looked at several different solutions and selected Symantec Data Loss Prevention met Banjercito’s business requirements. The Banjercito team began with a proof of concept during which they were able to verify functionality. The integration points with Security Information Manager and Control Compliance Suite were factors the Banjercito team took into consideration.

Just as Gutiérrez’ team collaborated with business owners to define compliance policies, they did the same around data loss issues. The entire process took about three months to complete. “The out-of-the-box policies in Data Loss Prevention were very useful,” Gutiérrez says. “As with our Control Compliance Suite deployment, these provided a solid starting point over which we were able to add custom-built policies specific to our business requirements. Since the business owners were involved in defining data loss prevention policies, they developed a sense of accountability.”

Working with a Symantec partner to scope and plan the implementation project, the Banjercito team oversaw the rollout of Data Loss Prevention across the organization’s network, endpoints, and storage. “The policies we developed specify different controls—from monitor to enforce—for the different data sets,” Gutiérrez explains. “We are able to manage our data loss risks based on business requirements.”

Proactive support
For help in managing its extensive Symantec investment, Banjercito relies on Symantec Business Critical Services. “Much of the technology we use is for business-critical functions and systems,” Gutiérrez says. “Security is a top priority for Banjercito, and we wanted to have a proactive approach to managing issues. And this is what we get with Business Critical Services.” Banjercito also uses Business Critical Services for the Symantec technologies used to enable the data center environment (see sidebar).

Business Critical Services has worked with Banjercito to resolve several different issues over the past year: “In one instance, we were receiving alerts of likely infected files on certain proprietary systems that we thought were false positives,” Gutiérrez says. “However, working with our Business Critical Services account manager, we found a way to efficiently confirm the level of real risk, fix the problem, and avoid the exposure of end users to such alerts. We could have spent hours trying to pinpoint the issue and then remediate it.”

Convergence engenders new opportunities
So to where is Banjercito headed next? Technology convergence is one area where Gutiérrez sees substantial opportunities. “We’ve already seen this with our security environment and the different technology pieces from Symantec,” Gutiérrez says. “They all work in concert with each other.”

But opportunities are broader in scope than in just security, according to Gutiérrez. For example, cloud computing and mobility both present substantial opportunities that are simply accentuated through the intertwining of technologies. “We’ll be looking at ways to take our existing investments and wrap new solutions around them for greater leverage and impact,” he concludes. “Enabling the bank to securely take advantage of cloud and mobility developments is certainly at the forefront of our radar.”

Patrick E. Spencer (Ph.D.) is the editor in chief and publisher for CIO Digest.

Banjercito leverages various Symantec technologies and services to protect its infrastructure and information at go.symantec.com/banjercito-video.