Chilean Bank Gets Proactive on Data Security After Cyberattacks Rock Latin America

A rash of cyberattacks in Latin America spurred this wealth management and corporate banking specialist to team up with Forcepoint to better protect sensitive data and its reputation among Chile's elite.

The government of Chile is in the process of enacting new cybersecurity regulations in the wake of 2018's high-profile cyberattacks targeting Latin American banks. This Chilean bank, which is charged with managing the finances and investments of its elite, high net worth individual and corporate clients, isn't waiting for those new rules to become the law. Turning to Forcepoint, the bank has proactively installed Data Loss Prevention (DLP) and Cloud Access Security Broker (CASB) to get ahead of whatever security threats crop up next.

CUSTOMER PROFILE:
Private bank founded in 1979 based in Santiago, Chile.

INDUSTRY:
Financial Services

HQ COUNTRY:
Chile

PRODUCT:
Forcepoint Data Loss Prevention
Forcepoint Cloud Access Security Broker (CASB)

In May 2018, Chile's second-largest bank, was robbed of about U.S. $10 million in a "smokescreen" type of attack. The attackers deployed destructive malware to infect the bank's workstations as a distraction while conducting a separate attack to steal the funds via fraudulent wire transfers. Similar attacks carried out in Mexico and elsewhere earlier in the year spurred the Chilean government to begin drafting legislation that will require Chile's banks to comply with certain cybersecurity measures, including data loss prevention.

This Chilean bank was not affected by the 2018 cyberattacks. Nevertheless, the private bank, primarily catering to high net worth individuals and corporations, decided to get proactive about bolstering its cybersecurity and data loss prevention posture. Instead of waiting for government regulations to take effect, it planned to get ahead of the curve to better protect clients and itself.

Keeping an elite clientele safe in the cloud

Founded in 1979, this Chilean bank and its subsidiaries offer an elite clientele a variety of top-notch, individually tailored financial services, including consumer, commercial, and investment banking services; wealth management, securities trading, and other brokerage services; and insurance products.

In recent years, the bank has been transitioning to the cloud to support remote bank employees and account managers who meet premier clients in their own environments. The bank needs its security solutions to both adhere to coming government data protection legislation and to safeguard the usage of cloud applications and service providers.

The bank is particularly concerned about employees using unsecure network connections to connect to the internet while working at remote locations.

> "Education and knowledge of the business, together with the appropriate technological tools, are essential to anticipating and preventing threats."
>
> BANK CISO

Forcepoint offers ease of integration, proactive approach

Though the bank was not affected at any time by the attacks on the financial industry, management made the decision in July 2018 to shift toward a more proactive approach that would anticipate possible threats and help prevent data breaches. The bank went with Forcepoint for both its data loss prevention and cloud application security needs in part because Forcepoint's solutions were more easily integrated into the bank's existing security framework than products from competing vendors.

Forcepoint's Data Loss Prevention (DLP) also met the bank's requirement for a solution with an educational component to train employees how to make data more secure through their own actions. This was facilitated through employee-coaching tools natively integrated into the DLP platform. Employees are empowered to self-remediate risk, giving them more flexibility to do their jobs without compromising regulated data.

"Our main challenge is to avoid or reduce information leakage. The key to this is understanding human behavior and how it can affect the company's data," said the bank's CISO. "The human factor is very difficult to predict. Education and knowledge of the business, together with the appropriate technological tools, are essential to anticipating and preventing threats."

Challenges

Prepare for coming government data protection legislation.

Safeguard the usage of cloud applications and service providers.

Approach

Implement Forcepoint DLP and CASB and tune as needed to evolving business needs.

Flexible data and cloud security that can be 'tuned' to business needs

On the cloud application security front, the bank went with Forcepoint's Cloud Access Security Broker (CASB). The CISO said the same ease-of-integration and educational factors informed the bank's choice, as well as a desire for a solution that would be 'tunable' to evolving business needs.

"When implementing Forcepoint CASB and DLP tools, we shifted the paradigm to understanding the rules of the business and translating that into the tool. This generates a control circuit that allows the tool to adjust to business needs—not the other way around," he said.

Forcepoint's approach gets closer to the interactions between humans and data, which further enhances the bank's commitment to being proactive about data security, added Forcepoint Account Manager Javier Chistik.

"The old static approach to security, which sought to only prohibit actions and put padlocks on things, is obsolete. Forcepoint helps companies better understand people's behavior with regards to handling data and how to look for behavioral clues to anticipate possible incidents," Chistik said.

Turning employees from security risks into data defenders

The bank has engaged Forcepoint Professional Services to fully integrate CASB and DLP. The DLP integration observes and flags risky data movement, while helping employees learn how their actions and decisions can either help safeguard the bank or create more risk.

"Internal training on this subject is essential and must be continuous. Generating awareness of how our actions modify essential data of the company is the first step, as well as training people on the proper use of tools. We live in a society where there are two cell phones per person, but we do not have a digital security culture in Chile," said the CISO.

Results

Observe and flag risky data movement, while helping employees learn how their actions can help safeguard the bank or create more risk.