CONVERGINT:

Electronic Security

EBOOK

convergint®

CONTENTS

Introduction

The banking universe has entered a remarkable era of enhanced accessibility, simplicity and convenience. As a result, most consumers would agree that both the digital and in-branch experience have been vastly improved.

But improved access has also created more risk for financial institutions, as practically every day, criminals target them with the intent to steal data and physical assets. Banks and credit unions can no longer rely on the branch defenses of yesterday. Proactive physical security infrastructure must include the very best in electronics, with regular updating to ensure optimal performance.

Whether updating or overhauling, electronic security can be a challenge for any financial institution given the pace of introductions and upgrades.

Not with Convergint. We have the means and methods to turn your cutting-edge electronic security integration aspirations into reality by recognizing your existing pain points and offering solutions for how to resolve them.

PAIN POINT NO. 1:

Danger at the Front Door

While technology surges ahead with the intent to enhance convenience and increase security, rogue nations and nefarious gangs are never far behind with increasing levels of sophistication, organization and focus on undermining FI defenses.

Based on the latest figures from FICO, there has been a 10% surge in the number of debit cards compromised at ATMs. Skimming and shimming are on the rise and increasingly sophisticated.

According to Positive Technologies, approximately **60% of attacks in 2019** were targeted in nature, meaning they were aimed at a specific vulnerability within an organization's infrastructure. Frequently, these attacks occur literally at the front door by sabotaging card entry readers.

Breaches of any kind not only lead to financial losses, but often result in diminished trust amongst account holders, most certainly for those who are directly affected. This, in turn, impacts overall reputation.

> There has been a **10% surge** in the number of debit cards compromised at ATMs.

SOLUTION:

A Layered Approach to Access Control

Basic, yet effective best practices are a critical first step for optimal protection. These include **mandating case-sensitive alphanumeric passwords, prompting regular password changes, and prioritizing access to only certain long-standing customers or tenured personnel.** That, however, must be complemented by advanced technologies to create a strategically layered defense.

Thanks to the proliferation of connected devices, machine-to-machine communication can systematize access authorization. A centralized access control solution from Convergint can accommodate existing access vestibules and deliver PCI compliance and universal control over all doors in your system. This ensures expedient response to any attempts at skimming or any unauthorized wireless entry.

PAIN POINT NO. 2:

The Deeper Security Threat

According to Cyber Security Insiders, the United States remains the number one target for cyberattacks, accounting for an astounding 54% of incidents. The banking space in particular is seriously compromised by this issue.

The cost of a cyberattack for a financial institution averages **$18.3 mil** per Accenture. Furthermore, a bank or credit union is **300 times** more likely to be attacked, and according to Carbon Black, **26%** of FIs have fallen victim. The results can be devastating when viruses weave their way into security equipment like DVRs and cameras. What are the steps that your institution can take?

The United States remains the number one target for cyberattacks, accounting for an astounding **54% of incidents.**

SOLUTION:

Line Up Your Defenses

> Proper protection of security equipment in the branch begins with the basics: **passwords.**

Proper protection of security equipment in the branch begins with the basics: passwords. Shockingly, too many DVRs and cameras are not properly set up with sophisticated password protection, nor are they updated regularly. Instead, Convergint has found that many FIs have equipment in place with out-of-the-box passwords – think PASSWORD – that are easily identified by attackers with just a google search or operators manual in-hand.

The first step in lining up your defenses is **proper password set-up and frequent updating for all DVRs and cameras.** The second? **Firmware maintenance.** Updating firmware is absolutely essential to data integrity, cyber-security and compliance. Furthermore, it ensures that the institution is leveraging all new functions and features, thereby justifying the technology investment. For these critical tasks, banks and credit unions have to choose between managing internally, outsourcing or combining the two.

PAIN POINT NO. 3:

The IT Investment

A layered approach to security includes access control, video and alarm; all integrated to optimize the protection of your branches. **This is not, however, without cost.**

Aside from the dollars and cents involved in equipment investments, FIs must dedicate staff to assist with implementation and maintenance. IT departments especially can be overwhelmed with upfront demands, further exacerbated by the constant need to install the firmware and software upgrades so critical to maintaining the value of the original investment and security in the branches while complying with stringent FFIEC requirements and other regulations. This, however, is complicated given their need to balance other priorities.

Aside from the dollars and cents involved in equipment investments, FIs must **dedicate staff to assist with implementation and maintenance.**

SOLUTION:

Managed Services

This is what makes managed services a smarter, more cost-effective security strategy. Hiring a third-party vendor to handle both installation and ongoing maintenance, including firmware updates, allows your institution to optimize your electronic security solution without having to worry about diversifying existing resources.

Letting go of the controls can create trepidation for many financial institutions; **luckily, you don't have to.**

A successful partnership with your managed services provider will necessitate the appointment of IT leaders for oversight and guidance. The time dedicated to this role will be much less granular and all-consuming as the 'do it yourself' option and will ensure **vendor transparency and accountability.**

PAIN POINT NO. 4:

The Pace of Technological Obsolescence and Preparing for the Future

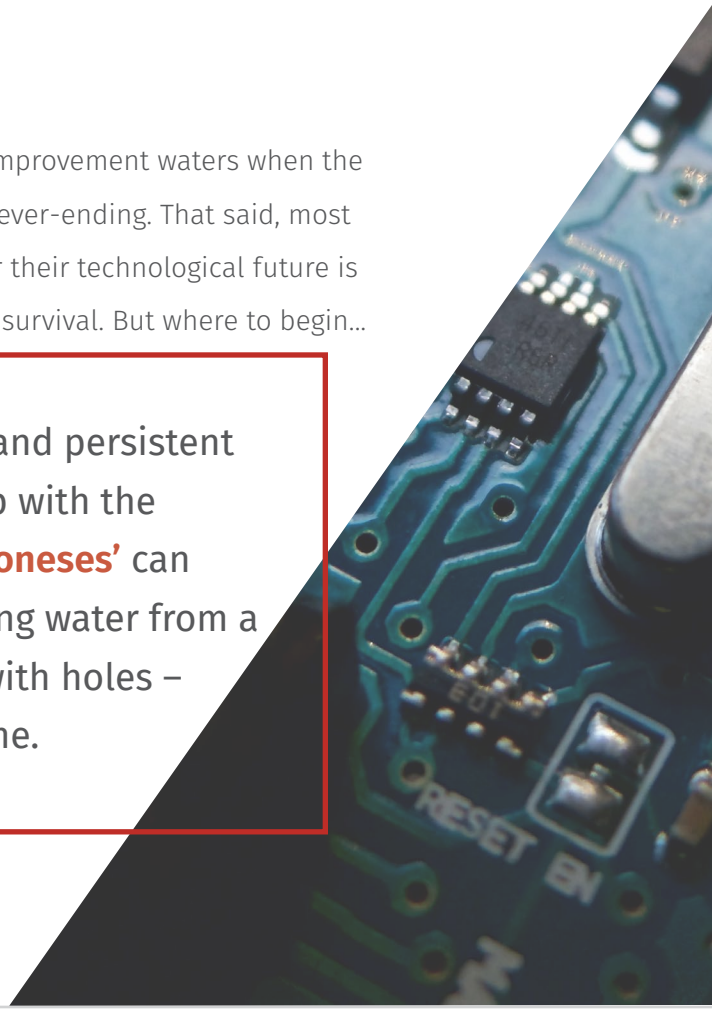
While the speed with which technology evolves is truly astounding, it can also be overwhelming.

We live in an age of the next big thing. Almost as soon as the latest version of a software, program, platform or device is unveiled to the public, it's not long before its bigger and better successor replaces it, rendering what was previously state-of-the-art to legacy status.

The consistent and persistent need to keep up with the 'technological Joneses' can feel like removing water from a rowboat filled with holes – one pail at a time. Despite your best efforts to stay afloat, it's ultimately a losing battle.

It may have some questioning whether they should even bother wading into technological improvement waters when the tidal waves of change are never-ending. That said, most recognize that preparing for their technological future is critical to their institution's survival. But where to begin...

The consistent and persistent need to keep up with the **'technological Joneses'** can feel like removing water from a rowboat filled with holes – one pail at a time.



SOLUTION:

Three Points of Focus

Future-proofing your electronic infrastructure can serve as your life raft to staying ahead of the hi-tech high tide. If nothing else, **focus on three things.**

1. **Migration** to IP is unquestionably important as this technology has proven time and time again to be superior in quality and scope of delivery.
2. **Remote access** gives designated personnel greater flexibility, controls and oversight in the areas of your facility that require round-the-clock monitoring via mobile devices, wearables and IoT equipment.
3. Most importantly, while not always easy, **Integration** is absolutely essential to the long-term viability of your total electronic security solution, and selecting an appropriate security platform can be a tremendous help. The right choice can mitigate threats, ensure compliance, and improve your investigations with advanced analytics. It can also facilitate significantly more streamlined upgrading procedures. But how can you choose a partner with low risk and high outcomes?

Convergint As Your Guide

Electronic security can be difficult to navigate all on your own. Convergint can help you steer the ship as your single point of contact for cutting-edge electronic security integration, including video surveillance, access control and alarm. Furthermore, we have multiple platforms to support optimal performance and an understanding that this is not a one-size-fits-all world.

Indeed, Convergint only represents best-in-breed products and can collaborate with you to develop a customized equipment solution that is an ideal fit for your institution. This is complemented by services including managed services, central station monitoring, repair and maintenance, decommissioning and more.

Embark on a successful electronic security integration journey with **Convergint as your first mate. Contact us today** to see why banks and credit unions nationwide choose us as their trusted navigator and guide.


convergint®