Ensuring Robust Security Measures: Insights from Intersect Las Vegas 2023

Security is critical when money is involved. While the attack methods and the intensity vary across geographies, criminals are developing new, sophisticated attack types with worrying speed. During Intersect Las Vegas 2023, ATM security was a leading topic discussed on both the main stage and during breakout sessions. Faced with a wide variety and constantly evolving attack methods, nearly 70 percent of attendees said their financial institutions experienced skimming AND physical attacks. Key banking leaders shared the steps they are taking to ensure continued security of their self-service channels.

Matt Snow
EVP, Head of Cash and ATM Operations
Regions Bank

Security updates are the thing I am most concerned about because of the change and pressure to continually maintain security with updates and patching. Less with physical security because we know how to do that in this space. It's digital security that concerns me more. Historically we patched our fleet two to four times a year, but now that is not even close to being acceptable. Today, we are talking about 10 to 12 or more in some cases. Unfortunately, that's simply basic security patching, not functional enhancements, not ProBase improvements or all the other things you really need to do to manage your fleet. So, balancing that and learning how to do that efficiently is one of the key challenges for our business. Thankfully, we work with Diebold Nixdorf and they have helped us through that.

David Volbrecht
Branch Technology Support Director
Randolph Brooks Federal Credit Union

We implemented a third-party monitoring solution. We take those vulnerabilities it detects and address them internally if we can. For the rest, we rely on Diebold Nixdorf Managed Services for solutions. Sometimes we engage Managed Services to identify something that had not been addressed yet as DN seems to be on top of that.

A lot of it {security updates} is keeping up to date with software, which anybody in security can tell you is the most important part. So, it is important to get the business on board to support those efforts and address the concerns that we have that our monitoring tool identifies

Mike McCourt
Director, Card Services and ATM
Premier America Credit Union

To ensure ongoing security updates, we are adding the most up-to-date software to the ATMs. Additionally, we are adding anti-skimming devices and using ActivEdge™ card readers, DN's long-edge card reader. We are being proactive and are on the lookout for fraudsters.

Ken Justice
Senior VP ATMs
PNC

Attacks are increasing and evolving. They are not static and attention needs to be given to these risks on a regular basis. Risk assessment hygiene is very important. Threats evolve and change the risk ratings on the countermeasures. Be sure to keep aware of what's going on in the industry. Sign up for all notifications from various vendors. We stay engaged with suppliers and in tune with the industry to ensure we keep both our reputational risk as well as fraud losses at a minimum.

THE TAKEAWAY

An overall knowledge of attack trends is important, but understanding their own defenses can quickly help FIs assess whether a new threat may become relevant to them. Regular security assessments provide a roadmap to determine if and which updates or changes to the security infrastructure are needed in the short term and can help define a long-term strategy. Ensuring our customers' fleets and networks are secure is a priority for Diebold Nixdorf, so we offer FIs complimentary security assessments. Our experts can help FIs assess their current security strategy and how it holds up against the risk landscape in their area, as well as how they compare to competitors. During a complimentary assessment, more than one hundred security aspects of the self-service fleet are considered.

Contact your Diebold Nixdorf Account Manager to schedule your Security Assessment.