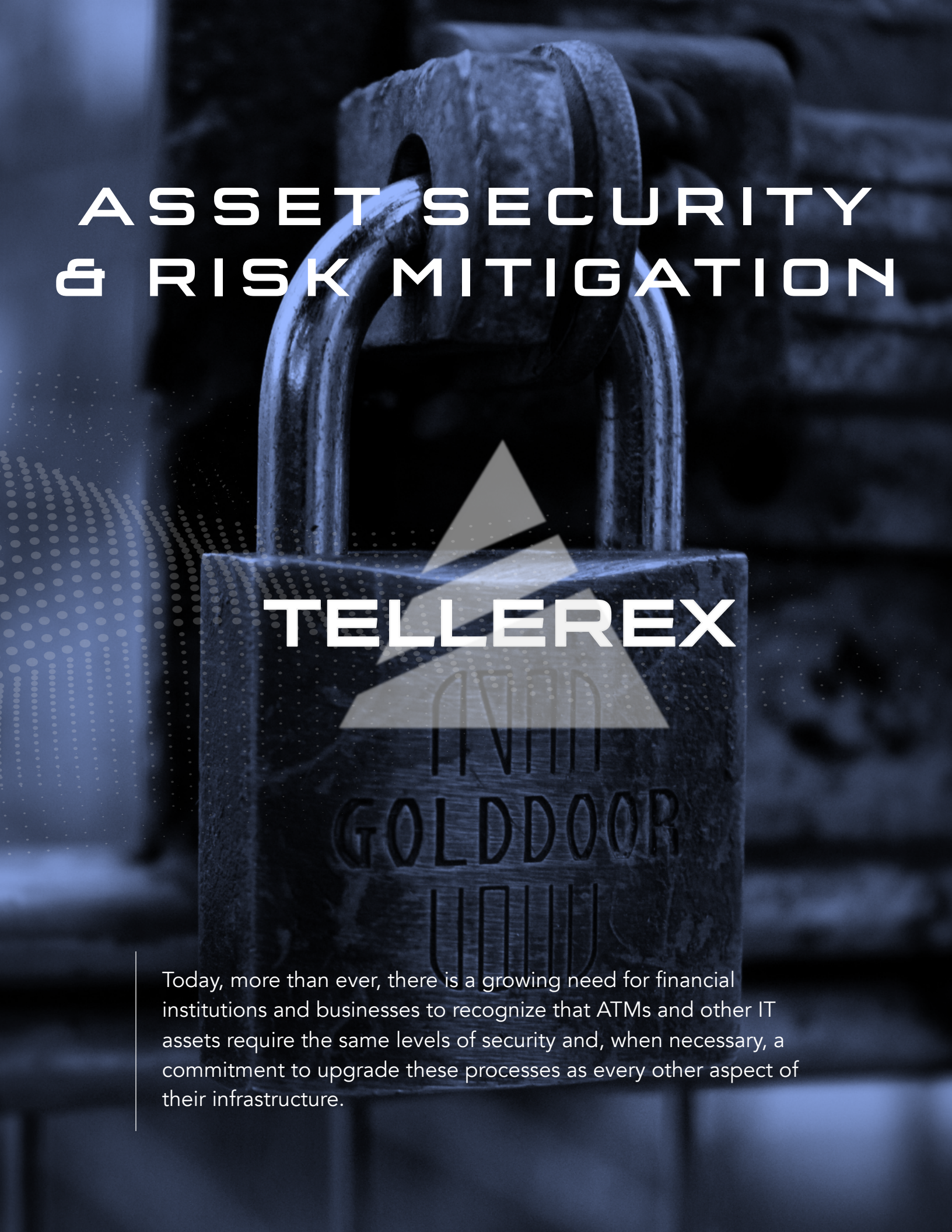


ASSET SECURITY & RISK MITIGATION

TELLEREX

Today, more than ever, there is a growing need for financial institutions and businesses to recognize that ATMs and other IT assets require the same levels of security and, when necessary, a commitment to upgrade these processes as every other aspect of their infrastructure.

TELLEREX

ASSET SECURITY & RISK MITIGATION

A COMPREHENSIVE GUIDE TO SECURING YOUR ATM & IT ASSETS

Consumers increasingly demand online and self-service financial products to support their on-the-go lifestyle. Is your financial institution prepared to ensure your customers' security for the future?

The financial services landscape is changing at a rapid rate, with financial institutions offering more access points than ever before. Consumers are driving this digitization because they want the convenience of being able to conduct their financial matters on any platform they choose, at any time they want.

To compete in today's marketplace, FIs may feel pressure to adopt new technology quickly. While adding new technology benefits both FIs and their customers, it's important to remember that institutional security must remain the company's top priority.

A single data security breach has the potential to put your organization at serious risk for lawsuits, fines, damaging publicity, diminished corporate revenues, and even imprisonment for the individuals involved. This fact makes it critical that your organization's asset managers understand the issues involved and exercise due diligence in selecting outside partners to manage their asset disposal processes.

THE IMPACT OF DATA SECURITY BREACHES

While everyone understands the importance of maintaining security, a 2016 Forrester report suggests over one-quarter of bank executives did not feel confident in their organization's ability to manage and prevent an ATM security incident. Furthermore, in the same survey, forty-two percent said their ATM security challenges were due to, at least partially, having too many ATM brands and devices to manage.

RISK TO ATM'S AND OTHER IT ASSETS IS ON THE RISE

According to an ATM Industry Association (ATMIA) report

From 2018-2019, attacks on ATM's increased by

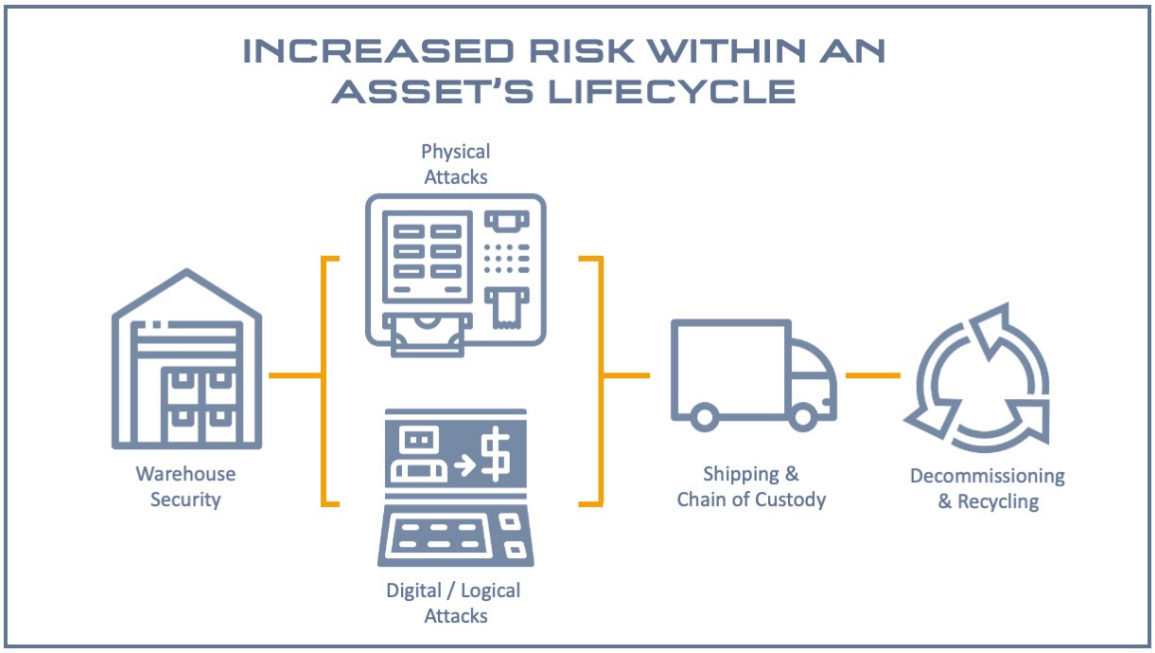
58%

$4M+

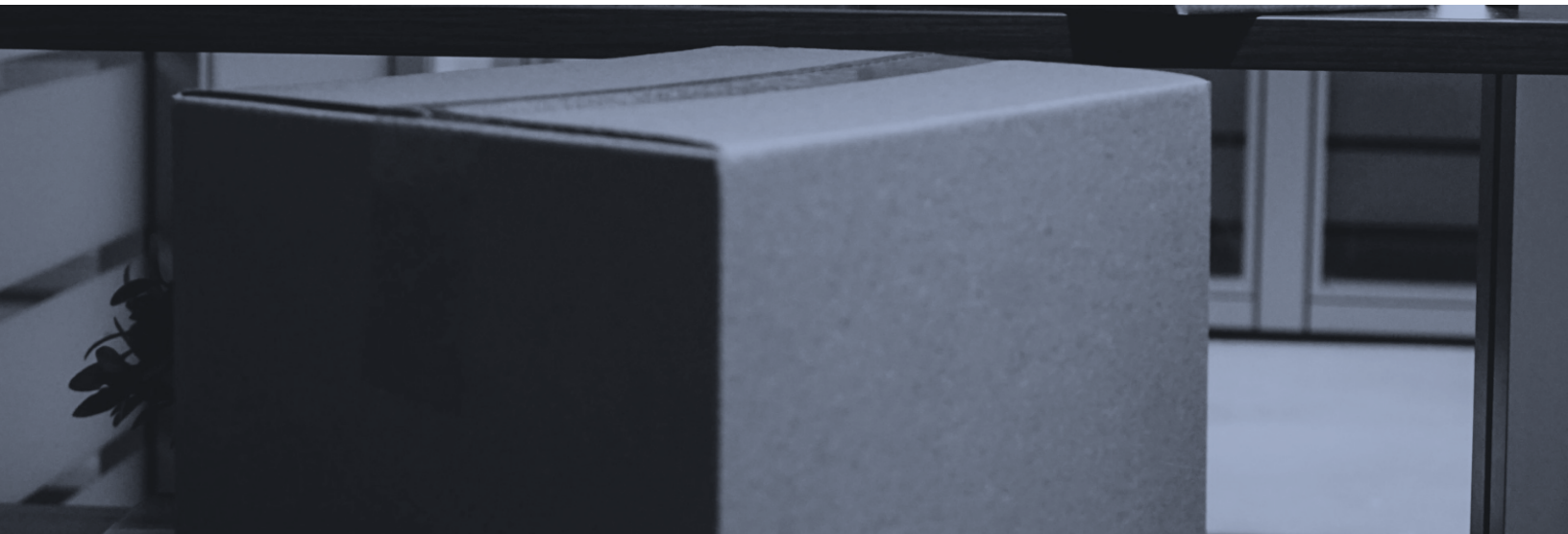
On average, the cost of a data security breach in 2018.

And this concern is well-placed. In 2018 a data security breach resulted in associated costs of, on average, over four million dollars. The ATM Industry Association (ATMIA) reported that overall, ATM attacks rose 58% from 2018-2019. With over 150 significant breaches per year, substantial money is thrown at a problem that many feel incapable of solving.

POINTS OF INCREASED RISK



- Shipping & Warehousing – Many overestimate the security of their storage facilities and the chain of custody processes.
- Physical Locations - Physical ATM attacks, focused on extracting cash, happen quickly and cause damage to ATMs.
- Cyber or Digital Components - Criminals are always looking for new ways to access cardholder data and to steal money from vulnerable ATMs.
- Decommissioning and Recycling - Regardless of its function, most asset disposal processes are overlooked. A report from Deloitte found 33 percent of IT executives admitted having little or no formal IT governance policies in place.



UNDERLYING PRESSURES

At the core of this issue are three primary trends that FI's must learn to counter:

1. How do you 'lockdown' channels while keeping accessibility high? – Providing optimal consumer experiences along with robust security measures are top priorities but can often feel in conflict.
2. In a competitive marketplace, increasing efficiency matters – A need for operational efficiency means more reliance on self-service banking. However, ATM security experts are scarce and represent a commitment of limited resources.
3. Finally, these circumstances lead to the most critical issue of all; Most ATMs are easy targets and can be hacked in under 20 mins, according to recent a report from PT Security.

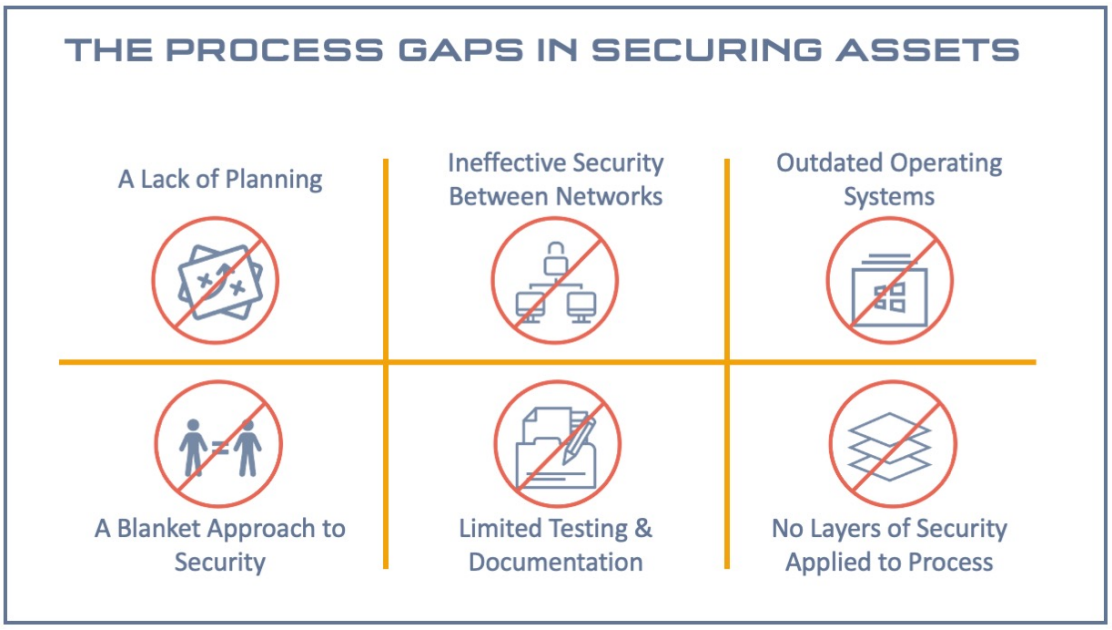
GAPS IN SECURING ATM'S

These breaches typically stem from a handful of crucial ATM network security gaps. Below are the most common across the financial industry. While these lapses can be eliminated, they facilitate easy unauthorized access to ATM networks if left unaddressed.

1. A Lack of Planning – Based on a 2017 PwC study, only 53% of companies maintain a proactive system (and data) management plan - fully, from the very start to the very end of the system's lifecycle.
2. Lack of Security Between Networks - To protect against ATM network security threats, financial institutions should install firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and antivirus software. Well-planned network architecture also requires the ATM network to be separate from the main one.
3. Outdated Operating Systems - ATMs running Windows XP leave ATM networks exposed due to the absence of patches for these outdated operating systems.
4. Applying A Blanket Approach to Security - Financial institutions often treat their ATM's all the same, implementing the same measures on every terminal, regardless of location,

age, or usage. A better solution is to conduct an analysis to determine which terminals are high-risk and allocate your limited funds accordingly.

5. A Lack of Documentation and Testing – When it comes to planning, many associates aren't sure what to do in the immediate aftermath of a breach attempt. Every bank should go through a mock attack exercise, so they can see how and where the triggers happen — or not— to understand what they need to do in the case of a security issue.



THE NEED FOR A TRUSTED PARTNERSHIP

In evaluating your organization's ability to protect assets, ask yourself the following questions:

1. Do we have in-house security experts knowledgeable enough to defend our self-service channel?
2. Do they have the time to keep up with evolving attacks and industry standards?
3. Do we have self-service security personnel struggling to manage the entire fleet?
4. Do we have a roadmap in place to maintain and upgrade our fleet security measures?
5. Do we know what type of attacks and defensive measures are coming next?

If the answer to any of these questions is no, it may be beneficial to look to an outside partner for assistance.

Today, more than ever, there is a need for banks and businesses to recognize that ATMs require the same levels of security and a commitment to upgrade, when necessary, as every other aspect of their infrastructure.

ABOUT TELLEREX

Tellerex is committed to leveraging our knowledge and experience to reduce atm expenses, increase reliability, and accelerate a contribution to your company's bottom line. Contact us to learn how our complete ATM management solution can simplify the end-to-end process and required oversight for your ATM and cash recycler networks.