WITTENBACH

ATM CYBERSECURITY THREATS ON THE RISE

ATM attacks continue to escalate across the United States and globally, with threat actors employing a broad spectrum of tactics—ranging from brute-force physical intrusions to highly sophisticated cyber-based exploits. Given the evolving threat landscape, there is no single solution capable of securing an entire ATM fleet against all potential vulnerabilities.

To mitigate risk effectively, a multi-layered security approach is essential. Implementing a combination of physical, logical, and network-based countermeasures significantly enhances the resilience of your ATM infrastructure and reduces the likelihood of financial and reputational loss.

WITTENBACH

Physical Security Measures

- Replace standard factory locks on the Topper, Fascia, and Beauty Doors with unique high-security locks
- Upgrade any unit (not already equipped) with safe reinforcement (to inhibit "Hook and Chain" attack)
- Use Bollards and Security Gates (to inhibit "Hook and Chain" attack)
- Use Card Readers with Anti-Shimming plates installed

Electronic Security Measures

- Alarm the top section of the ATM
- Add Siren and Strobe Lights in the top section of the ATM
- Consider additional camera coverage of the ATM
- Use Card Readers with Anti-Skimming technology

Software Protection

- Activate MoniGuard Encryption on the ATM Hard Drive
- Configure MoniGuard Whitelisting to block unauthorized software
- Review and deploy current software levels (MoniAct, MoniPlus) as available from Hyosung to maintain updated security features
- Install Windows security patches as available
- Change access passwords (Winlock, Supervisor, etc.) from factory default

ATM Network and Communication Security

- Enable TLS (Transport Layer Security) protocol to secure network communication
- Firewalls should be actively maintained

FI Preventive Measures

Since technology alone cannot guarantee effectiveness against all forms of ATM cyberattack, it is also recommended to perform a routine, even daily, inspection of the ATM.

- Look for any new stickers, labels, or plastic items
- Inspect that all fascia components are weathered "evenly"
- Look for unusual scratches around the card reader or key locks
- Wiggle the card reader to assure that it is secure and check for other loose parts on the fascia
- Can a card be easily inserted into the reader?
- Scrutinize external lighting fixtures and mirrors on or around the fascia
- Does the keypad look and feel "normal?" (could suggest the presence of an overlay)
- Check for any small holes in the fascia or ATM trim work (opening for a pinhole camera)
- Is the lighting around the ATM adequate?
- Are cameras positioned appropriately and focused

ATM Managed Services

- Ensures that all software is uniform across the ATM fleet
- Remotely deploys Windows security patches to all units
- Verifies appropriate software levels are installed
- Can remotely update/change passwords
- Can remotely set dispense limits
- Monitors ATM activities and may defect unusual or criminal activity

CONTACT US TODAY

800-638-8618
sales@wittenbach.com
wittenbach.com