

VILLIGER SECURITY PERSPECTIVE

Five success factors for physical ATM protection

By Andy Villiger, VILLIGER SECURITY

Do you know the total cost of one ATM attack on your network? What about five attacks within three months? The exact figure is not easy to calculate, but the reality is that the overall costs are much higher than at first we are led to believe – say three times, five times or more. To find your specific figure, form a team of different stakeholders from within your ATM network: technical services, finance, marketing, insurance, security, CIT and

maybe even customers.

Then have this team work out price tags for all factors below the surface, such as cost of downtime, loss of image, total repair efforts, effects on insurance, and so on. The total cost will surely justify measures to reduce the risk of physical ATM attacks. But which measures to choose? To help you decide and to provide you with some ideas from our experience in protecting ATMs around the world, I list here five success factors that would highly leverage every investment in ATM security.

1: Focus on prevention

Our primary goal is not to catch the bad guy after an attack, but to prevent the crime in the first place! Firstly, check your security measures in relation to their preventative effect against professional thieves. What makes criminals go elsewhere? Psychology tells us what bad guys do not like: risk of failure, aggressive colours, change, waiting, uncertainty, traceability and additional stress. Secondly, take action before you suffer from attacks. Risk analysis is an ongoing, forward-looking process.

2: Take the bad guy's view

If you are responsible for doing risk analysis, here is an effective and eye-opening tool. Switch your brain to 'attack-preparation' mode. Leave the office for a few hours, or even a week, and be a careful observer. Evaluate all possible targets for an attack. Change your 'brutality level' with the different amounts of money at stake. And include insider know-how, because this knowledge is used in 95% of all attacks worldwide. Now switch back to 'banker mode' again. What have you learned? The bottom line of your in-depth study will be that bad guys prefer the most attractive targets AND you should make your ATMs less attractive targets. And DO announce your protection measures with meaningful plates.

3: Use robust technology

Ink-staining products installed in ATM cassettes are a highly effective protection measure which has produced impressive anti-robbery statistics. Several manufacturers offer products for nearly all ATM brands. You may find significant differences regarding robustness, ease of use for CIT, scalability and total costs. It is up to you to choose the right partner. This is an important decision.

4: Be a team player

To maximise security and minimise costs, collaboration between eight parties is needed: yourself, insurer, national bank, CIT operator, police, government, ink protection partner and any retailers providing sites for your ATMs. Teamwork within this group will enable you to maximise the effectiveness of your security investments.

5: Guarantee an ROI > 300%

Last but not least, investments in security must be justified. Use the team of stakeholders noted earlier and test different factors in your calculations. The results will cause your CFO to have sleepless nights. It's time to ask for the VILLIGER ROI Checklist! ■

av@villiger-security.ch

