VULNERABILITY OF ELECTRONIC SECURITY GRID & RESPONSES

Introduction

An electronic surveillance cum security grid is seen as the next generation system which supplements and in some cases even replaces the ubiquitous guard. The facilities for remote screening, documenting for evidence and analysis by a combination of Closed Circuit Television (CCTV) networks for 24/7 surveillance of desired areas has meant that the systems are in place today in every place of public interest. A combination of surveillance, identity, access controls and so on can provide an unobtrusive network which is being preferred especially for business entities which have large footfall of regular employees or customers. At the same time an electronic security grid is vulnerable and thus complete reliance on the same is ill advised with preference for an integrated electronic cum physical guarding systems. The focus of the paper is however only on vulnerability of electronic security grid as the integrated system has been covered separately.

Aim

The aim of this Paper is to identify the vulnerability of electronic security devices in asset guarding and grid and suggest suitable responses for the same.

Electronic Security Grids

Electronic security grid facilitates non proximate guarding replacing or supplementing trained personnel by cameras and other electronic devices for monitoring of activity at a given location. A common electronic security grid today could include one or more of the following – CCTV/ Internet Protocol (IP) Video Surveillance cameras, electronically operated gates, barriers or turnstiles, intruder and other alarms such as fire, remote control access, identity verification devices and for large facilities even UAVs and Drones. Connecting the devices in a network using big data analytics and geo-intelligence can provide real time view of security over entire facility on a single screen. Thus adoption of electronic devices for security such as CCTV cameras in a grid has been all pervasive. There is some vulnerability however which need to be taken into account and mitigated.

Common vulnerabilities

The common vulnerabilities of electronic security grid apart from the physical damage that a miscreant can cause are summarized as given below. These include vulnerabilities of systems as a whole as well as that of individual devices.

→ Lack of awareness of the risk posed to electronic security systems in India is a major hazard. Once a system is installed it is believed that it is secure and will provide all information. It is only on occurrence of an incident are the challenges exposed.

→ Internet Protocol (IP) based security systems such as video surveillance cameras are run as standalone systems or in some cases integrated into the corporate IT network fully or partially. A standalone system is relatively safe and compromise requires direct targeting electronically, through cyber or physical means. Compromise of such a system will also not affect the IT network as a whole. A partially or fully connected system on the other hand is vulnerable from permeation of viruses that have

infected the main system and vice versa, thus implementation of such a system has to ensure that adequate safe guards are inbuilt to avoid a compromise.

→ To save costs systems that are not cyber hardened are used which can suffer outages due to inherent deficits or external targeting.

→ Weak passwords, open ports, outdated firmware, lack of certified cryptography and so on are some of the common loopholes that have been noticed in electronic grids.

→ Cyber attackers can use a variety of techniques to infiltrate a system. They are proficient in targeting even through smart phones and can inject viruses including Trojans, worms, and spyware to compromise stored data and disrupt functioning.

→ Cyber intrusions could be the first stage of penetration which can facilitate physical entry to miscreants.

→ Ransom ware is a new threat that has emerged which can comprise the system and lead to payment of heavy demands through bit coins.

→ Identity recognition systems can be compromised by the use of fake access cards.

→ Power outage is a physical threat to systems

→ Many times user agencies have been known to switch off a system due to power overload and to save costs, when the objective of these is to provide 24/7 surveillance

→ Local environmental factors can have an impact by reducing efficiency due to low light conditions or be impacted by electric discharge such as lighting unless adequately protected.

→ Electronic or surveillance fatigue sets in early due to limitations of human monitoring of CCTV or other surveillance networks and thus those detailed to monitor may miss out on vital information.

Vulnerability Mitigation

Measures for vulnerability mitigation are outlined as follows:-

→ Prepare a SOP specifically for ensuring the security of the electronic surveillance grid which should include persons responsible for operation, maintenance procedures to prevent compromise and on. Where a system is password protected the frequency for change along with password generation software should be incorporated. Responsibility for security of the electronic systems has to be fixed in the SOP.

→ Cyber hardening of the system has to be ensured in concert with experts in this domain and should not be left to personnel who have acquired knowledge on the job even if the same leads to increased costs.

→ Physical security of log in and password is important, frequently this is stored on the mobile phone and miscreants will invariably target the same to obtain the information.

→ Any new entrant attempting to access the network, change password or configuration should send an alert to ensure that in case the system is compromised relevant persons are notified and can take immediate action to prevent further damage.

→ Ensure high level of cyber security hardening and in selection of a system choose one which has inbuilt security features which are self-renewable based on fixed time frequencies.

→ Under normal circumstances it may be difficult to identify the type of vulnerability, whether it is simply a system hang due to minor issues or a more serious Denial of Service (DDos) attack. Thus expert advice should be obtained earliest.

→ Training of operating personnel to differentiate between DDOS attacks and minor infringements with means to rectify the same as soon as possible is necessary.

→ Personnel should be trained in scheduled maintenance. For large complexes the services could be sourced to the systems provider who can place his technicians on site along with adequate tools to detect and rectify the faults.

→ Regular turnover of personnel detailed for monitoring is necessary to avoid electronic or surveillance fatigue.

→ Emergency power backup to cover the expected down time should be ensured.

Conclusion

Integrated manned and electronic guarding can overcome some but not all the deficits in cyber based systems that have been mentioned herein. While integrated guarding may be one solution there is a need to also implement measures to mitigate vulnerability of electronic grid separately which has been covered herein.