Is Technology the Future of Security?

Security is the preservation of life and protection of assets & data against malicious damage or theft. It continues to evolve and counter emerging crime trends. Technology continues to redefine the security landscape like never before. It provides for the deployment of intelligent equipment working alongside human beings as a complement or entirely on its own. This enhances security as technology covers the “blind spots” too.

Why Technology?

Aspects of human life including security, need periodic improvements to guarantee continuity in the most efficient way. Technology increases efficiency while narrowing down operation costs in due course. Nature of crime informs on the type of technology agent to be deployed to provide benefits in the security realm. The following are two major areas where technology continue to transform security;

1. **Physical Security**

   Entails deployment of intelligent equipment which can detect intrusion and alert for follow up action. A defined space like a home or office can be protected using a simple intruder alarm system. Laser beams are equally used to form protective rings around an area. These secure defined spaces against unwanted entry.

   Security entities increasingly use electronic devices for monitoring personnel patrol. Same are interfaced with surveillance cameras for various functions including monitoring, interpretation of facial and vehicles' number plate recognition technology.

   In some areas, smoke sensors detect signs of fire and trigger alarms or fire suppression measures. At other installations, it's for medical emergency alerts through panic buttons or sensors. Other security benefits include personnel screening using biometric systems and Metal & Baggage Scanners at entry points like airports. This equipment can “see” beyond the usual human eye, taking security to the next level.

2. **Cyber Security**

   It's a technology that provides security to stored data, information on traffic through networks, various storage devices like computers, servers and mobile devices. It's majorly proactive protection by use of applications like SIEM which alerts on the presence of cyber-attack agents like computer viruses and triggers a countermeasure by decoding malicious code which forms the intrusion. This then neutralizes the

attack. Incidentally, all systems all over the world are vulnerable to cyber-attack until proper measures are put in place. Cyber Security is further explained as follows;

I. *Application Security*

Security is provided through formulated measures that are designed to ensure that both soft and hardware parts of a computer are secure majorly at the development level. Dry-run like SAST is conducted after completion to gauge vulnerability and advise on any further required technological mitigation.

II. *Information Security*

It's data protection while in storage or on transit against unauthorized access, recording, and malicious use or destruction.

III. *Operation Security*

Advice on handling, protection and permission protocols for network access and storage. The process informs on action against data threats, gaps and corresponding mitigation measures like Endpoint Detection and Response Security.

IV. *Network Security*

The action of securing computer networks through configurations against intended or opportunistic exploits. Several technological measures have been developed to counter spear phishing which has been on the rise. Antimalware solutions and other security multilayer defences are some of the countermeasures used in mitigation.

V. *Disaster Recovery and Business Continuity*

A strategy for technological security response for revamping operations after a damaging event or outage. Equally meant to ensure operations are taken back to the same capacity even without full resources.

VI. *End-User Education*

The network can be penetrated using innocent users like employees. Education and security system communication can be installed as a program that runs on the screen as instructed. It reminds you of the dos and don'ts like, "delete suspicious email attachments and No plugging in of unidentified USB."

Conclusion

Technology is already a serious security pillar and poised to gain more ground in the future. Days that human beings were the only face of security are steadily waning away. More effective, consistent and less expensive deployment through technology is fast taking over. This affirms that technology is the future of security.