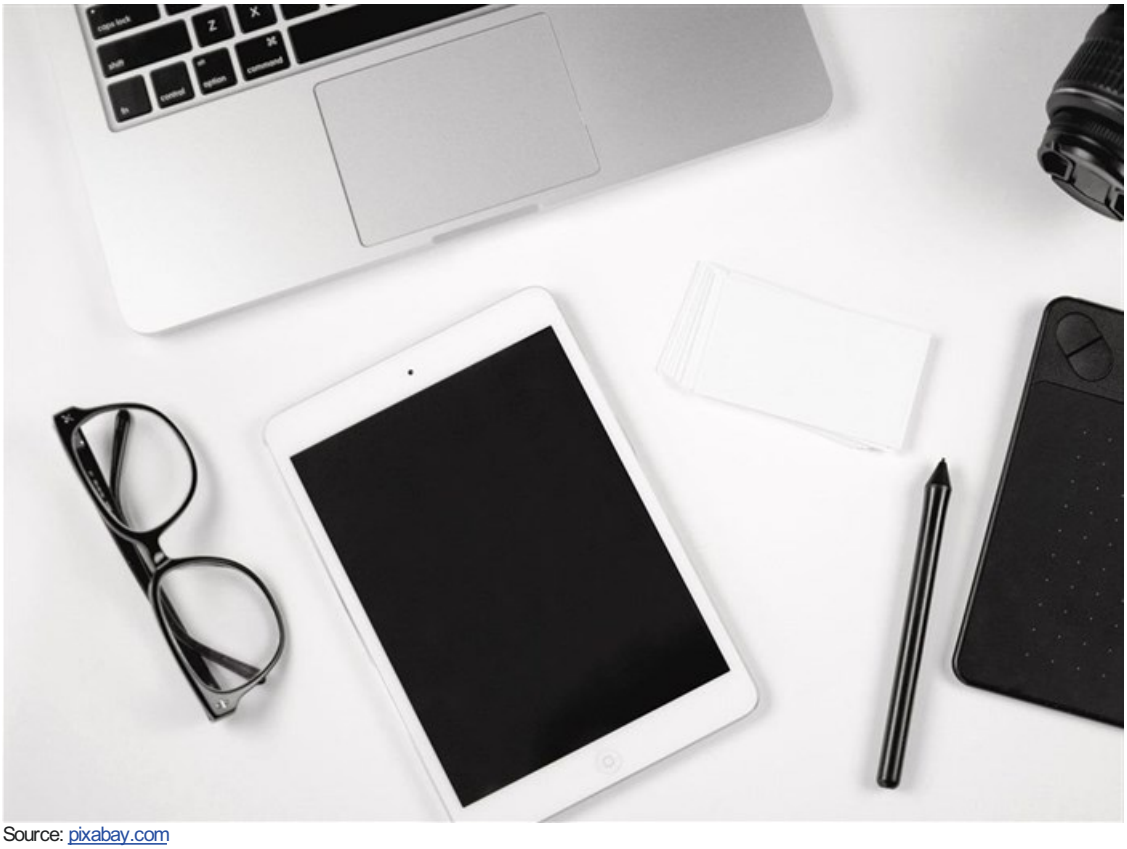
# How to protect IoT devices in your business

A guide for businesses to secure themselves against pervasive IoT-linked cybercrime.



Source: pixabay.com

The internet of things (IoT) is making its presence felt in a big way. It is expected that there will be 29 billion connected devices by 2022. This opens a whole world of opportunities for businesses to cement their relevance by evolving how they operate.

It also exposes them to the ever more ubiquitous risk of IoT-related cybercrime. In fact, the average total cost of cybercrime is estimated to be US$13m, representing an increase of 12% since 2017.

IoT is a network of devices, appliances and vehicles, for example, that are able to connect and exchange data.

“All IoT device-connected businesses are susceptible to cyberattack, and therefore by implication cybercrime. Failure to implement security controls and creating awareness amongst end-users are still the leading causes”, says Grant Durr, SOA

and security technology specialist at Santam.

This was evident in the widely reported Orvibo data breach last year, where approximately 2 billion records were exposed in a massive smart home device breach.

Considering the prevalent IoT security challenges, excessive data breach threats and constantly growing cybercrime, businesses need to adopt IoT security protocols and techniques to ensure the protection of valuable information.

Here are important provisions businesses can put in place to protect themselves:

- **Implementing best-practice cloud controls**: Organisations which use ISP (Internet Service Provider) hosting platforms or cloud providers should ensure that best practice cloud security controls are considered and adopted. Cloud security controls are countermeasures that are intended to avoid, detect, counteract or otherwise minimise security risks to information.

- **Ensure your servers are up-to-date and are running anti-malware software**: Running an anti-malware program on your server is a smart decision. Without one, you run the risk of having malware spread from one computer to all computers on your network. Keeping your servers and workstations up to date with the latest security patches will help to minimise the chance that a known vulnerability can be exploited which could lead to a data breach, malware infection or ransomware attack.

- **Provide cybersecurity awareness training to employees**: The most common cyber-attacks reported by companies are malware, phishing, man-in-the-middle, denial-of-service and credential reuse. Providing cybersecurity awareness training for staff is, therefore, a must for every business.

  Any device connected to a corporate data network represents a potential attack vector. It is imperative that employees understand the importance of adhering to basic security practices such as using strong passwords, social engineering awareness and regularly updating their software.

“With the reward of innovation comes greater risk”, concludes Durr.