DEVICE RISKS

The explosion in the production and adoption of internet of things (IoT) devices has meant that implementing proper security within the software, firmware and hardware has become a complex and often neglected task. Cybercriminals can obtain access to confidential corporate data within minutes through hacking a connected device, but it can take days, weeks or even months to remediate

DEVICES YOU DIDN'T REALISE WERE A POSSIBLE SECURITY RISK

🟥 DISASTROUS
Potential for irreversible damage and an invasion of user privacy, gaining access to private corporate information or destroying critical equipment.

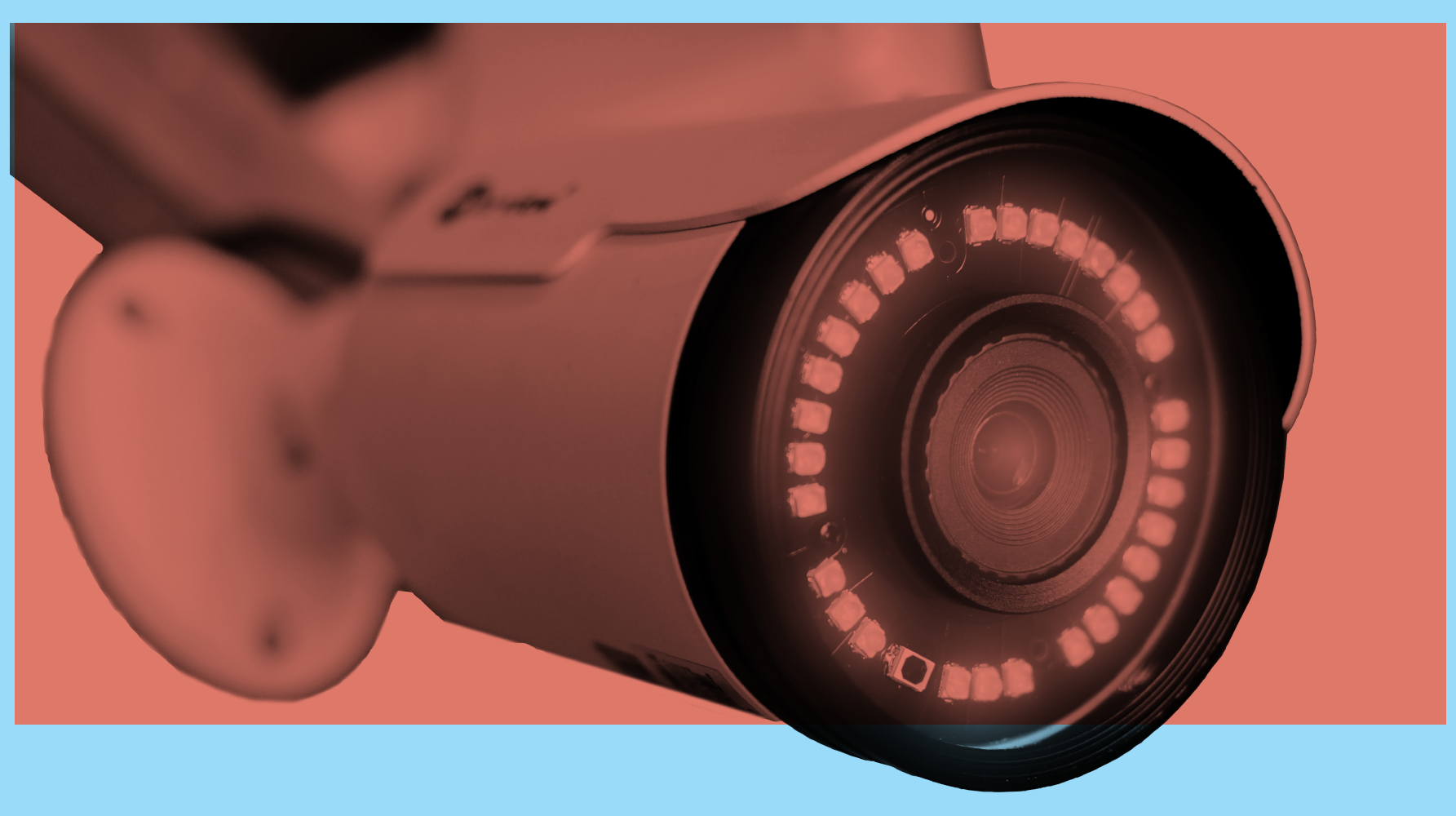
🟧 DISRUPTIVE
Could disrupt corporate and operational processes.

🟦 DAMAGING
Would allow snooping around a corporate network or extracting private credentials.

🟥 DISASTROUS

IP-CONNECTED SECURITY SYSTEMS

Many wireless security cameras use radio-frequency technology that lacks authentication and encryption, and attackers can form radio signals to send false triggers and access system controls. Radio signals are easy to detect and are open to jamming and spoofing, which could allow criminals to turn off motion sensors, remotely open locks, or redirect or switch off surveillance equipment.



🟧 DISRUPTIVE

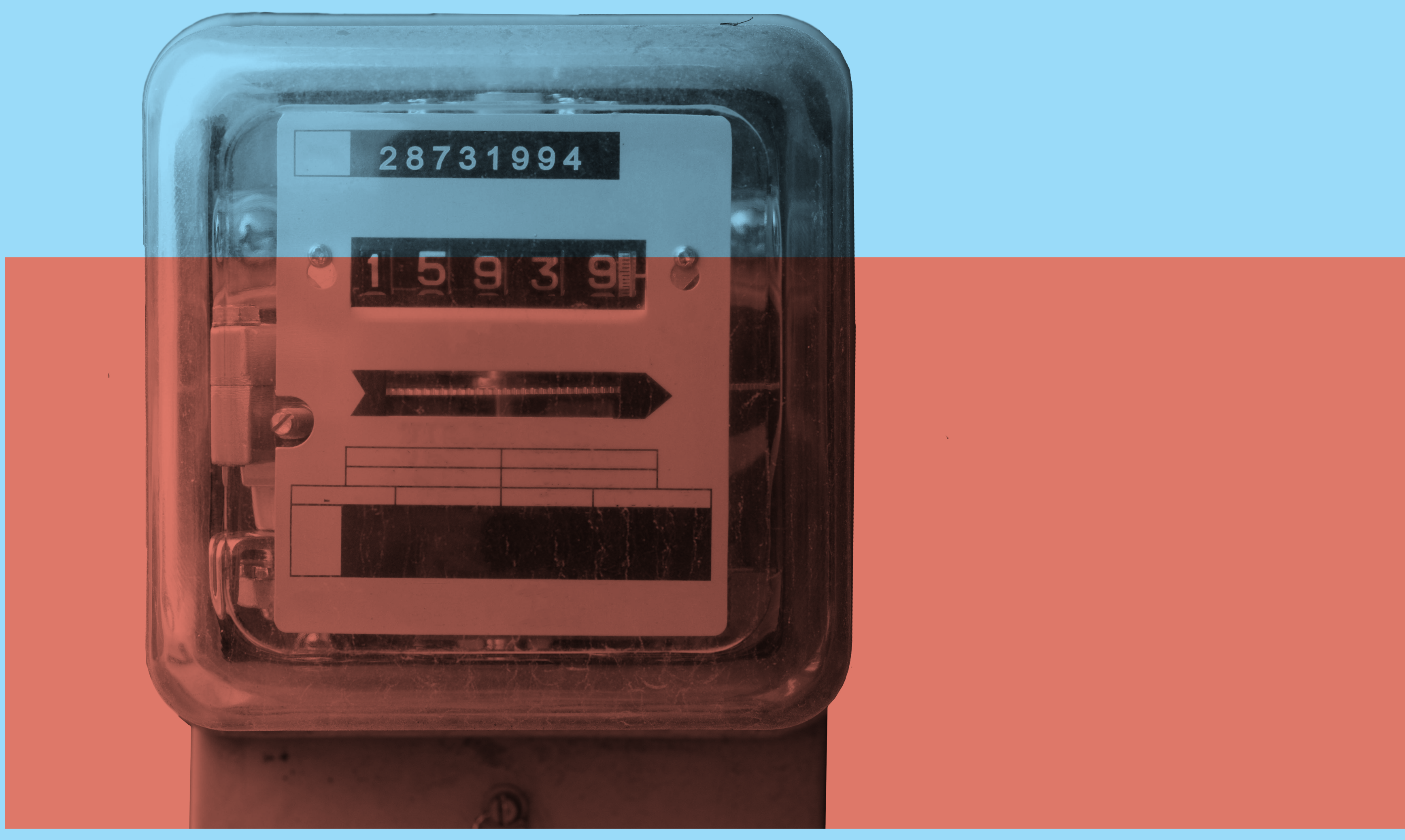
SMART VIDEO CONFERENCE SYSTEMS

Online streaming, conference calling and screen-sharing can be easy pickings for hackers, who can take control of any apps on the system, such as social communication, audio and video. At the same time, hackers have access to sensitive places, such as boardrooms and C-level offices, not often accessible by outsiders. Furthermore, most systems use common operating systems, which have overflow vulnerabilities, so they could be accessible from behind a router or firewall.

🟥 DISASTROUS

IP-CONNECTED INFRASTRUCTURE – CLIMATE CONTROL AND ENERGY METERS

Heating, ventilation and air conditioning equipment is typically connected to the same network as internal systems, which hackers can easily access to intercept data and carry out further attacks. Attackers can force areas such as server rooms to overheat and cause physical damage, while hacked smart energy meters can alter the reported energy levels of a company, potentially leading to fraudulent accounting and metering.



🟦 DAMAGING

SMART LIGHTBULBS

Smart lightbulbs operate on wi-fi and proprietary mesh networks, which can easily integrate into other connected systems that can be controlled by external devices and hackers. Mesh network communication channels can be "sniffed", so attackers only need to be within wi-fi range of the smart bulb with no original access to the network. Hackers can extract password-protected wi-fi credentials, allowing them to gain access to other systems and devices in the enterprise.

🟦 DAMAGING

SMART FRIDGES

Wi-fi-enabled fridges with LCD screens have access to widely used operational apps such as schedules, calendars and notification systems, and the credentials stored within. Due to lax certificate checking, attackers on the same network could conduct a man-in-the-middle attack to intercept communication and modify traffic between a client and server. This can be done by injecting spoofed address resolution protocol requests or domain name system responses.

🟧 DISRUPTIVE

CONNECTED PRINTERS

Nearly all printers are networked over IP or internet protocol, making them accessible from virtually any computer on the network. Hackers are able to siphon printed documents, which is almost undetectable without proper security and monitoring. If printers are on a public network or attackers are on the same wi-fi, they can send a specially crafted simple network management protocol packet to obtain the admin password and gain full control of the printer. Many exploits are not resolvable without updates to firmware or an intrusion detection system.

🟧 DISRUPTIVE

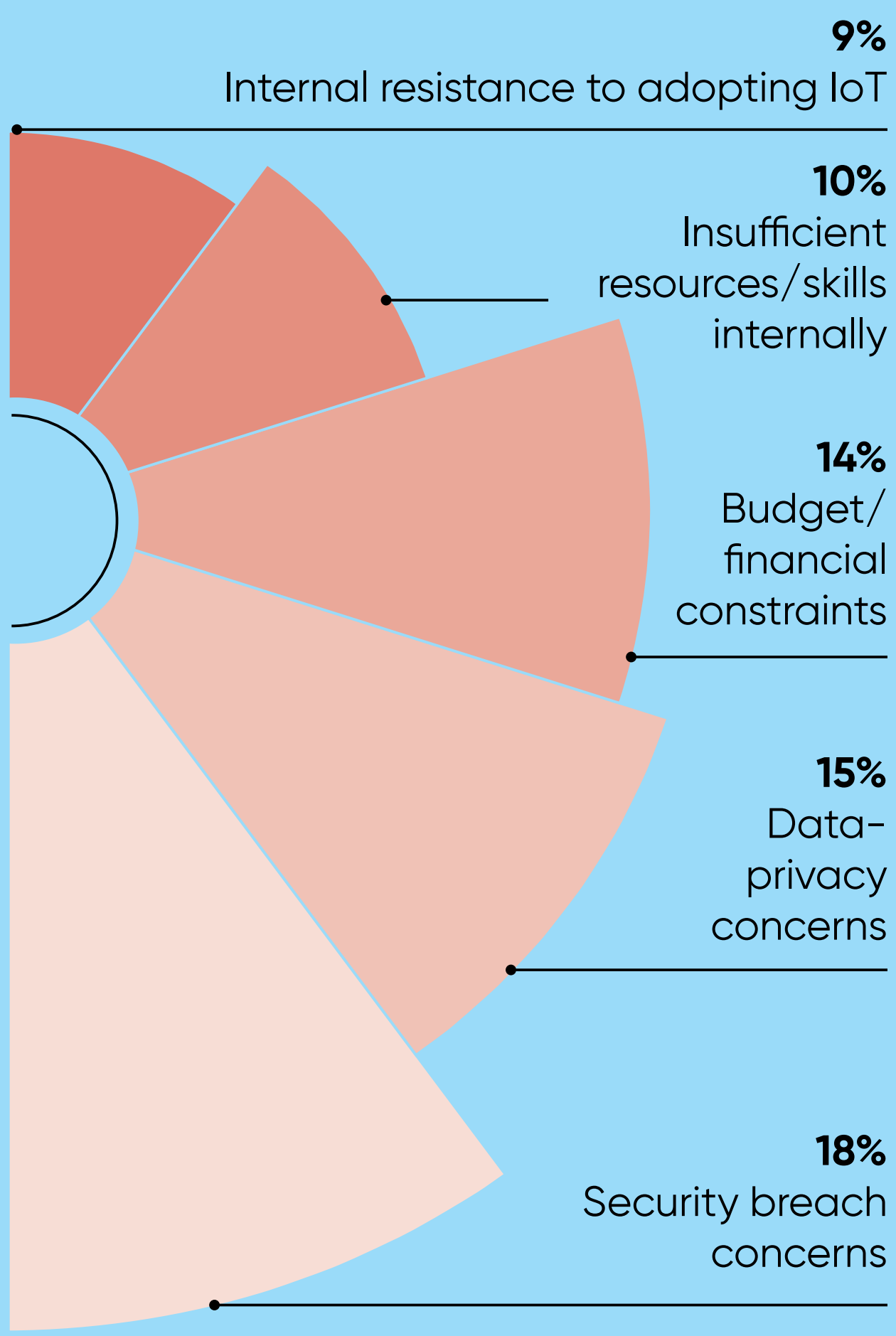
VOICE OVER IP PHONES

So-called VoIP phones leverage the network for many sophisticated features that makes communication easy, not only for employees, but also malicious hackers, who only need to know the phone's IP address to access it. Some can be activated as a speakerphone with no visible indication, while hackers can exploit configuration settings to evade authentication and then update the phone, allowing them to listen to conversations or make calls.

ForeScout 2016

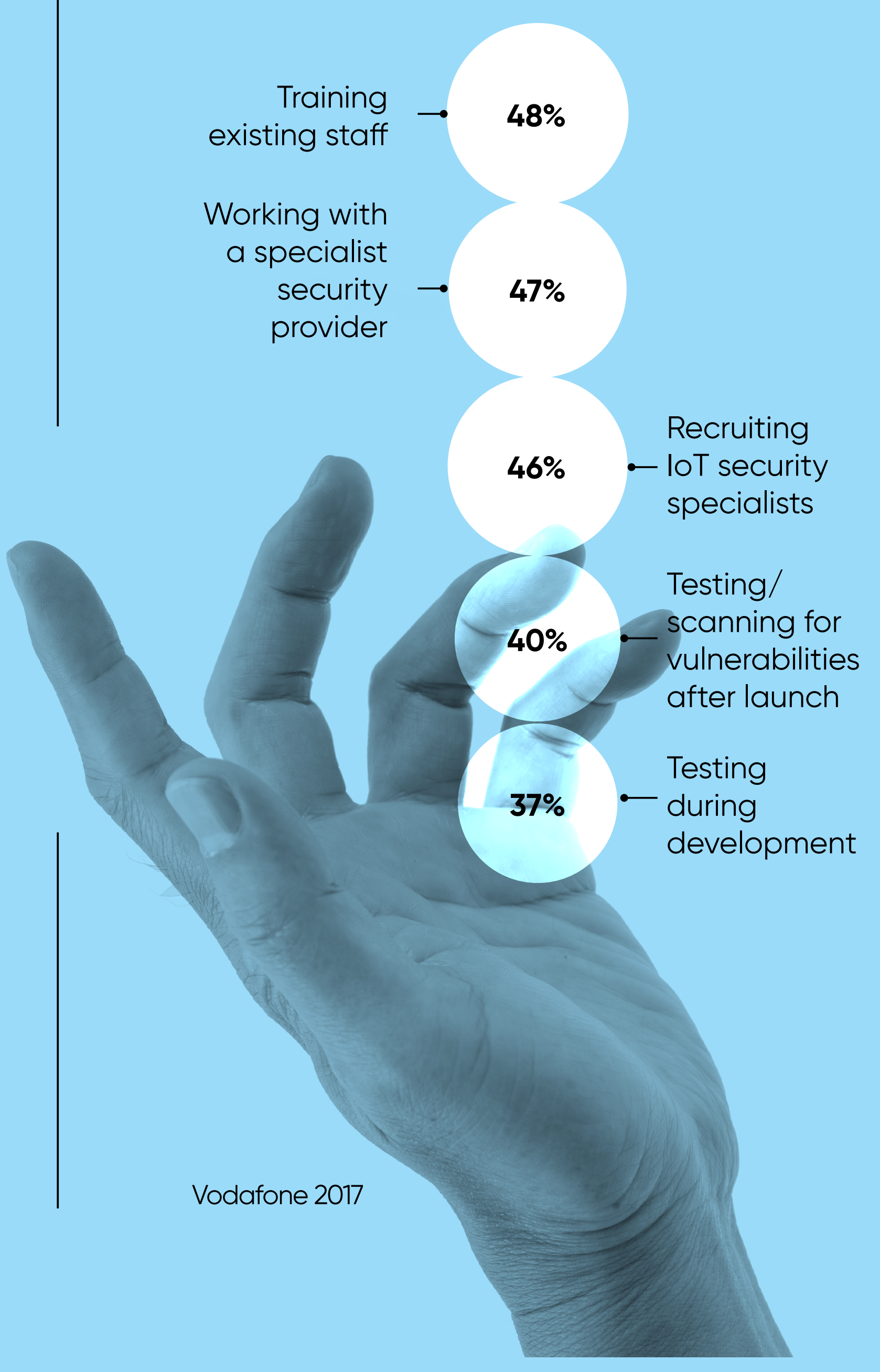
BIGGEST BARRIERS TO FURTHER IoT ADOPTION

Global survey of cross-industry decision-makers



WHAT ORGANISATIONS ARE DOING TO IMPROVE IoT SECURITY

Global survey of cross-industry decision-makers



Vodafone 2017

RACONTEUR