5 STEPS TO CREATING A SECURE BLUETOOTH ENVIRONMENT FOR YOUR TWO-WAY RADIOS

THE EXPLOSIVE GROWTH OF BLUETOOTH

Bluetooth technology is everywhere. Originally devised to replace cables, Bluetooth has evolved from the short-range wireless connectivity standard into something much bigger. Since it was first developed in 1994, over 9 billion devices have been shipped and, as every second passes, more than 57 Bluetooth-enabled devices are released to the consumer and enterprise markets.

OVERVIEW

Fast, secure and always-on communications. These fundamental principles of mission-critical communications underpin the design of reliable two-way radios that provide a lifeline for frontline staff. With the increasing adoption of Bluetooth-enabled two-way radios, organisations need to invest in technologies that combine the usability benefits of wireless connectivity with uncompromising performance. Making the wrong choices can result in serious information security breaches and communication failures with potentially life-threatening consequences.

BY FOLLOWING FIVE STEPS, YOU CAN CREATE A MISSION-CRITICAL BLUETOOTH ENVIRONMENT FOR YOUR TWO-WAY RADIOS AND MITIGATE THESE RISKS

STEP 1 Ensure that all wireless devices support Bluetooth V2.1 or later.

STEP 2 Implement a white list of trusted devices in all Bluetooth-enabled radios.

STEP 3 Always pair Bluetooth audio accessories with radios that integrate fast wireless push-to-talk.

STEP 4 Ensure that Bluetooth devices are powered by batteries with sufficient capacity to support a 10 hour work shift, based on the dominant usage profile.

STEP 5 Ensure that Bluetooth headsets have been designed to minimise the mouth-to-microphone distance.

THIS WHITE PAPER PROVIDES THE BASIS FOR THE FIVE COUNTERMEASURES BY HIGHLIGHTING IMPORTANT SECURITY AND SAFETY RISKS THAT MUST BE ADDRESSED WHEN DEPLOYING BLUETOOTH-ENABLED TWO-WAY RADIOS.

KEEPING US SAFE

A reliable and secure communications link is the critical factor, particularly in public services where Bluetooth is used in countless applications to make personnel safer and organisations more efficient.

KEEPING OFFICERS SAFE IN COVERT OPERATIONS

Bluetooth-enabled communication devices can be concealed more effectively, keeping undercover officers in constant contact with backup.

HELPING PARAMEDICS TO DELIVER EFFICIENT PATIENT CARE

Bluetooth connectivity allows paramedics to operate and communicate more efficiently without the constraints of radio cabling.

TRACKING LONE WORKERS IN INDOOR ENVIRONMENTS

When endangered workers don't respond to a scheduled communication request, a network of Bluetooth beacons can notify the rescue team of the worker's precise location.

MONITORING THE HEALTH OF FIREFIGHTERS

By coupling body sensors with Bluetooth-enabled two-way radios, incident commanders can monitor real-time vital signs to check the health status of their firefighters.

WITHOUT RELIABILITY, THE LIVES OF PUBLIC SAFETY PROFESSIONALS AND THE PEOPLE THEY SERVE ARE PUT AT RISK

ALWAYS RELIABLE
ALWAYS SECURE
ALWAYS ON

So what does security and reliability mean in the case of Bluetooth? It means creating a mission-critical operating environment by ensuring secure, fast and always-on communications.

Based on research and our experience working with public safety organisations, we're sharing five practical countermeasures that you can use to create a mission-critical, secure Bluetooth environment.

Let's first review the technology and some of the key security enhancements that have been implemented so far.

BLUETOOTH SECURITY: A BRIEF HISTORY

In the early days of the Bluetooth standard, headsets were shipped with strong personal identification numbers (PINs) and all Bluetooth versions used the same pairing process. Yet in the consumer market, pairing issues became the single largest source of customer service calls. While longer PINs increased the security of the pairing process, the administrative overhead of managing PIN information in a multi-user enterprise setting was significant.

To fix the usability issue, manufacturers opted for simple 4-digit PINs such as "0000" or "1234", making it easier for pairing to be automated. But this opened up a security weakness in v2.0 and earlier devices, as attackers could easily detect the Bluetooth PIN. Automatic pairing meant that they could pair the device before the legitimate user, gaining unauthorised access to data and eavesdropping on communications.

Security attacks were highlighted in the mainstream media, and these vulnerabilities led to Bluetooth being perceived as insecure.

With v2.1, things changed. A new pairing mechanism called Secure Simple Pairing (SSP) was introduced to fix all of the security issues of the previous pairing method without sacrificing usability. Here's the crucial difference. With SSP, even if a hacker knows the PIN, he is not able to decrypt communications over the Bluetooth link – the encryption algorithm in v2.1 is fully independent of the PIN.

KEY FACTS ABOUT BLUETOOTH

Bluetooth is a wireless technology standard for short-range communications, operating in the globally unlicensed 2.4 GHz industrial, scientific and medical (ISM) radio band. The purpose of the standard is to provide a common communication medium for a wide range of devices from different industries, such as computers, mobile phones and low power body-worn sensors.

Different power classes of Bluetooth device exist. The most popular, such as earpieces, support transmission distances of up to 10 metres. The effective transmission range varies due to radio propagation, antenna configuration and receiver design.

Bluetooth security has been designed for mission critical users who need to focus on the task in hand, not the technology.

FROM STRENGTH TO STRENGTH

Like all wireless technologies, Bluetooth will be susceptible to a range of security vulnerabilities. Such flaws can subject a user to a diverse set of threats, such as eavesdropping, Man-in-the-Middle (MITM) and denial of service attacks.

The good news is that by putting in place a mission-critical operational framework for Bluetooth devices, we can successfully counter threats. The first step in implementing this framework is to ensure secure Bluetooth connections.

ENSURE SECURE BLUETOOTH CONNECTIONS

Among the most serious attacks against wireless technologies are those that result in the loss of confidentiality and data integrity. Specifically, the key security threats here are eavesdropping and man-in-the-middle attacks. To ensure secure Bluetooth connections, these threats must be eradicated.

Critical to preventing eavesdropping is eliminating all possibility of an attacker discovering the link key, which is generated in the device pairing process.

By ensuring that all Bluetooth devices support Secure Simple Pairing (SSP), available in Bluetooth v2.1 devices, robust security against eavesdropping is assured.

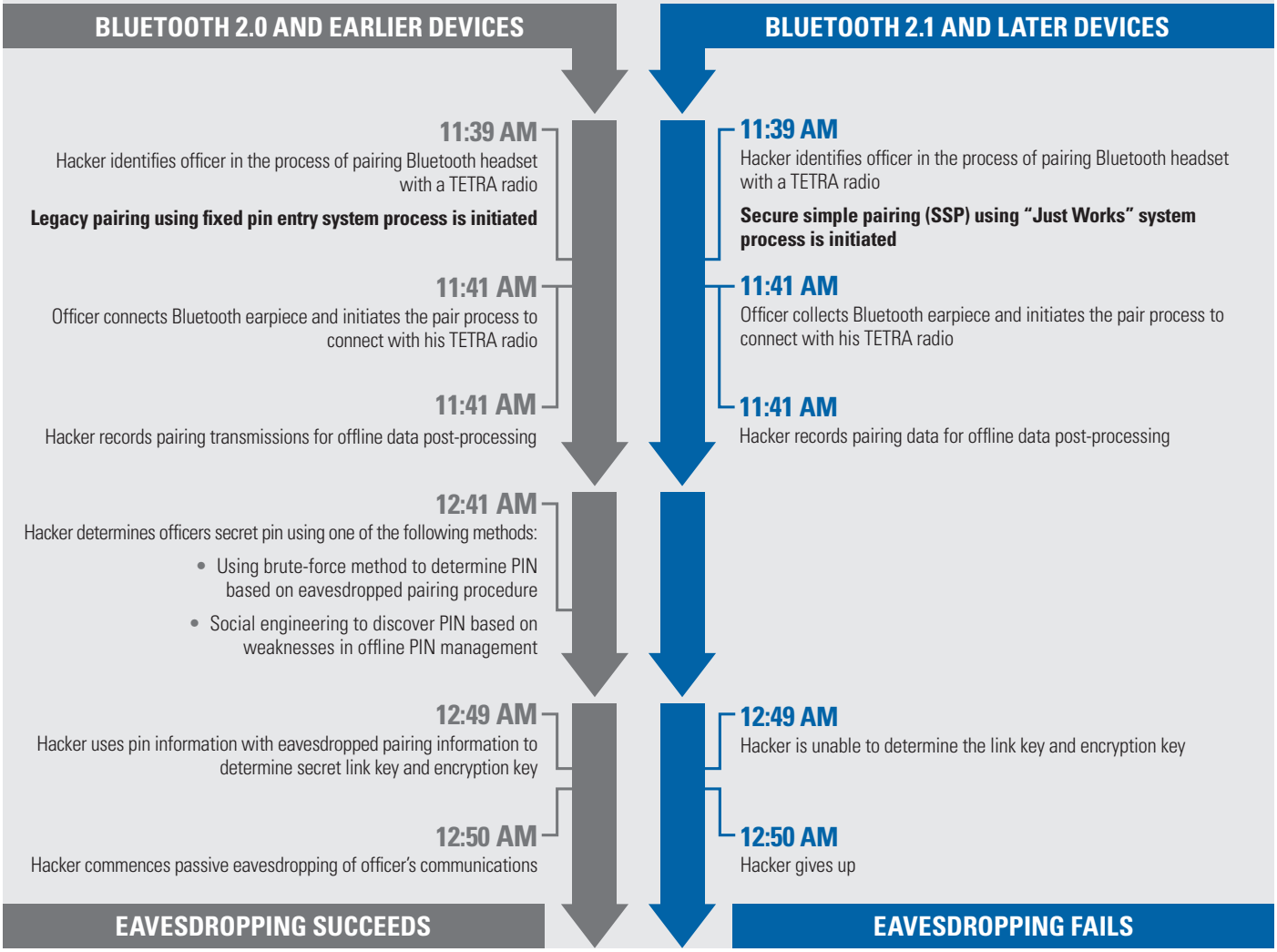
1 COUNTERMEASURE EAVESDROPPING

ENSURE THAT ALL WIRELESS DEVICES SUPPORT BLUETOOTH V2.1 OR LATER

In addition to eavesdropping, a determined adversary might choose to launch a MITM attack. This occurs when a user unknowingly connects to an attacking device that's playing the role of the legitimate device. The hacker can eavesdrop on the two devices, interrupt and mimic the authentic communication, and control operation of the valid devices to the extent that they only work when the attacking party is within range. This threat has caused such concern that one of the key goals of the SSP protocol is to prevent MITM attacks.

SSP incorporates a number of protocols called association models to allow pairing between devices with varied input and display capabilities. In particular, the Just Works association model was designed for situations where one of the pairing devices has a limited user interface, as is the case with headsets. Just Works, however, doesn't offer MITM protection and extra security measures are needed, especially in mission critical applications.

SECURITY FLAWS THAT OPEN THE DOOR TO PASSIVE EAVESDROPPING



SECURE SIMPLE PAIRING AVAILABLE IN 2.1 IS CRITICAL TO PREVENTING EAVESDROPPING
WITH SSP, LINK KEY GENERATED IS NOT BASED ON PIN.

- SSP uses the Elliptic Curve Diffie-Helman key agreement with public/private key pairs to generate the secret link key.

2 COUNTERMEASURE MAN-IN-THE-MIDDLE

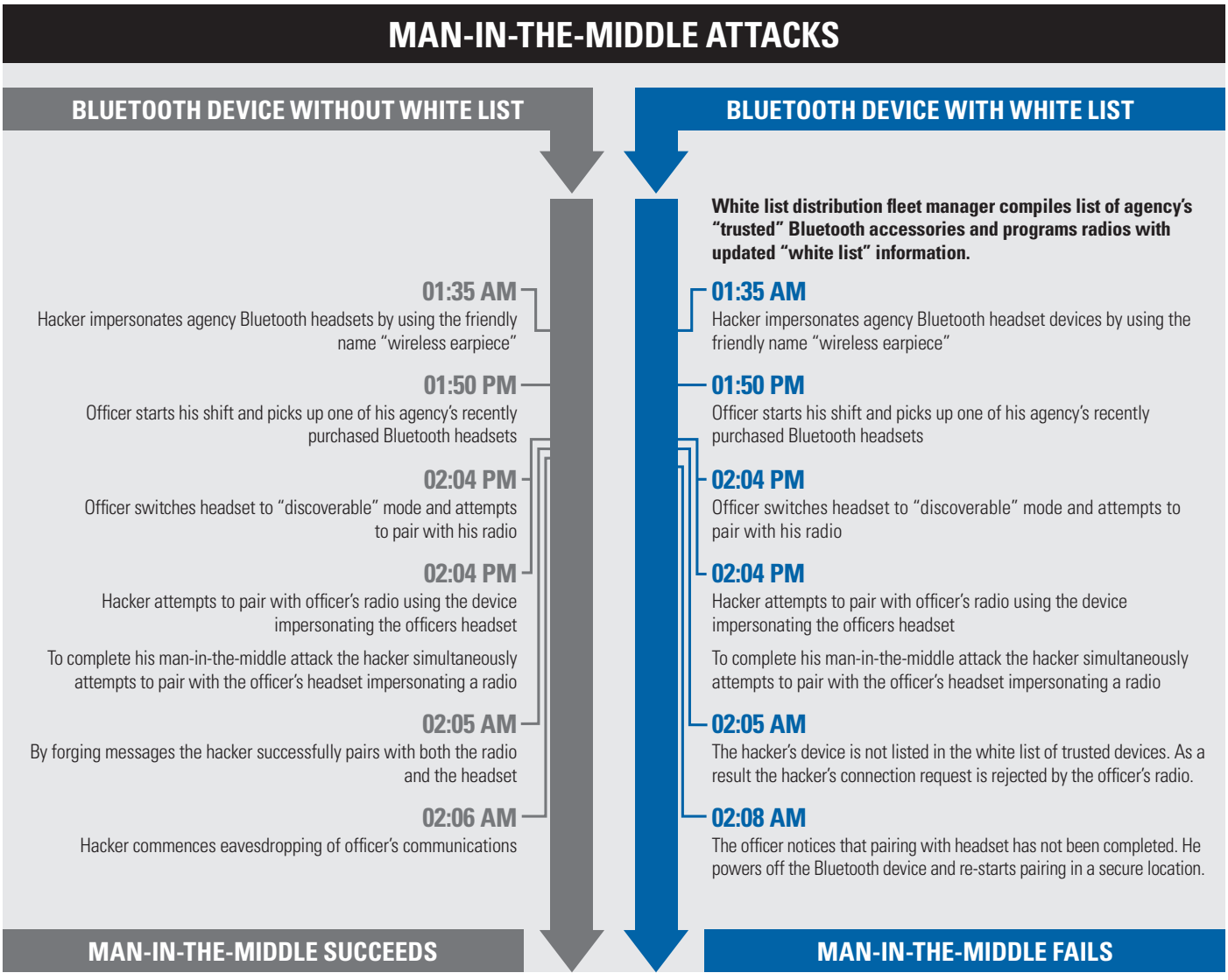
IMPLEMENT A WHITE LIST OF TRUSTED DEVICES IN ALL BLUETOOTH-ENABLED RADIOS

The first stage of the MITM attack is to capture enough information to impersonate the legitimate devices. Among the key pieces of information required is the unique Bluetooth device address (BD_ADDR) which is used to verify the identity of communicating devices. Paired with the BD_ADDR is a friendly name that appears on a device's display, to notify the user of devices that can be connected to.

IT'S EASY TO REDUCE THE RISK

To reduce the risk of impersonation through discovery of BD_ADDR, Bluetooth-enabled devices can be switched to the invisible setting (not discoverable). The friendly name field should be also set to non-descriptive. For example, manufacturer default friendly names should be avoided, as these are easily spoofed by a hacker.

We also recommend that you implement a list of trusted devices, also known as a white list. This ensures that a hacker can't stage an opportunistic MITM attack by spoofing the friendly name.



3 COUNTERMEASURE SLOW PUSH-TO-TALK (PTT) RESPONSIVENESS

ALWAYS PAIR BLUETOOTH AUDIO ACCESSORIES WITH RADIOS THAT INTEGRATE FAST WIRELESS PTT

In incident response, the difference between what's said and what's heard can be life-changing. Consider the impact of the command "Don't shoot!" being received as "Shoot!". To ensure the safety of radio users, immediate communication is vital. For this reason, low latency (delay) remains a core attribute of mission critical voice services demanded by public safety professionals.

YOU'RE HEARD. INSTANTLY

Based on a survey of professional users, mission-critical voice services must achieve call setup times of less than 500ms and end-to-end audio delays of less than 1s. These same requirements must be satisfied when Bluetooth audio is used.

RAPID RESPONSE

As the majority of Bluetooth devices operate on battery power, the standard includes important power-saving mechanisms to ensure extended operation. Sniff mode is one such mechanism for audio headsets. Sniff mode suspends Bluetooth radio communications between paired devices but maintains continuous contact, while listening for specific commands that occur periodically. It reduces battery power consumption in the radio and in the headset as the receiver can be put into standby between sniff cycles.

However, there is a flip side to the power saving. Push-to-talk (PTT) requires an immediate response and the scheduled transmission absences in sniff mode can also introduce delays in transmitting a PTT request to the radio. Depending on the manufacturer's setting of the sniff_interval parameter, delays of greater than 500ms can be introduced, decreasing PTT button responsiveness and potentially endangering the user.

For mission critical applications, Bluetooth audio connections need to be configured to:

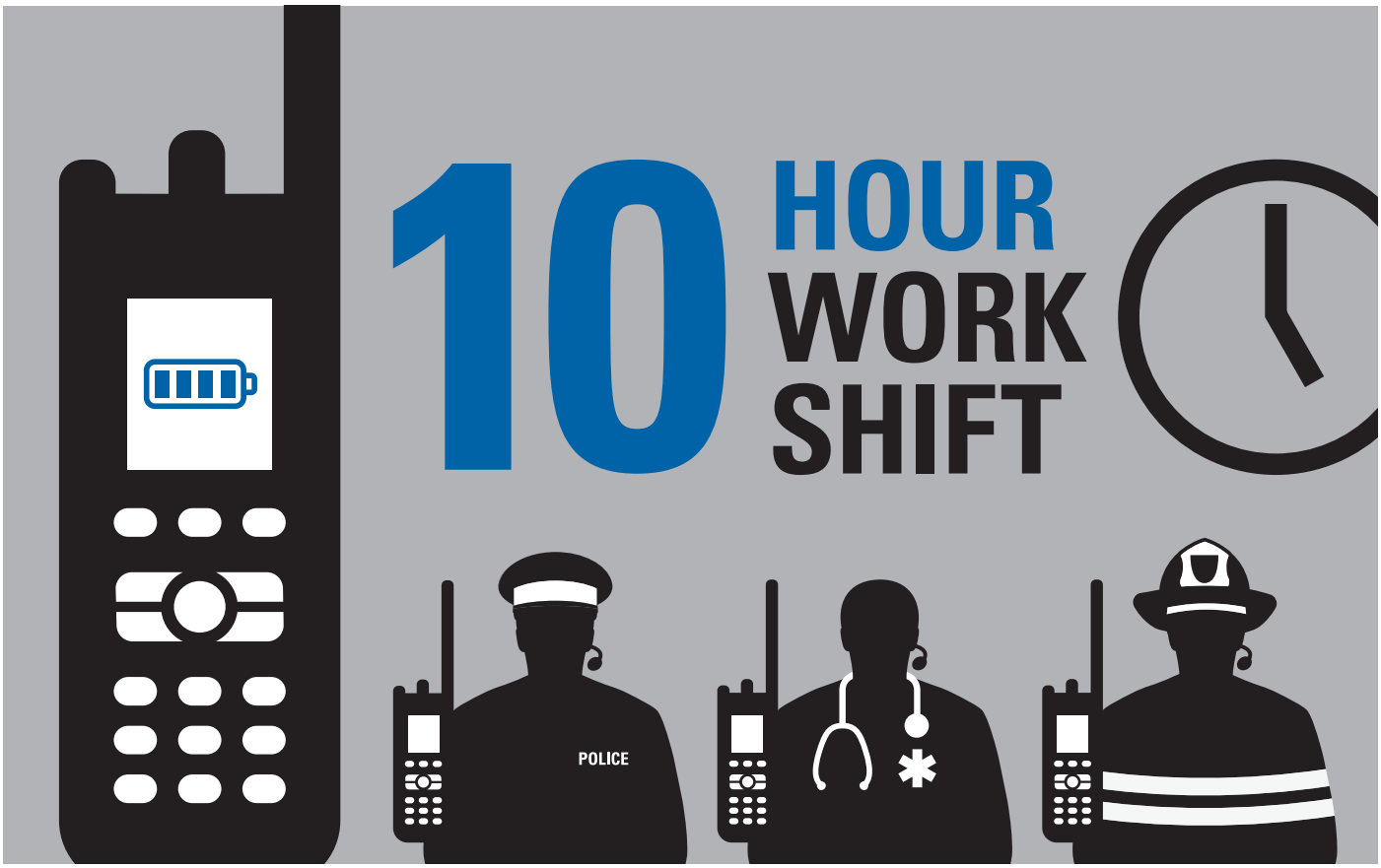
- Maximise PTT Responsiveness
- Guarantee Very Short Call Setup Times
- Minimise Transmission Delays

We strongly encourage you to select a vendor with mechanisms to minimise the variability in PTT response times, while ensuring extended battery operation.

4 COUNTERMEASURE REDUCED OPERATIONAL TIME

ENSURE THAT BLUETOOTH DEVICES ARE POWERED BY BATTERIES WITH SUFFICIENT CAPACITY TO SUPPORT A 10 HOUR WORK SHIFT, BASED ON THE DOMINANT USAGE PROFILE

Clearly, ensuring reduced power consumption and maintaining always-on connectivity are conflicting requirements. To address this trade-off, it's important that Bluetooth devices are designed with enough battery capacity to cover at least 10 hours of continuous operation, a typical duration for a work shift. The battery capacity must also support the dominant usage profiles among your agency's radio users.



5 COUNTERMEASURE BACKGROUND NOISE

ENSURE THAT BLUETOOTH HEADSETS HAVE BEEN DESIGNED TO MINIMISE THE MOUTH-TO-MICROPHONE DISTANCE

Of equal importance to extended battery operation is ensuring that audio quality is not compromised by Bluetooth connections. For a connection to be defined as 'available', audio messages must be intelligible to both speaker and listener, especially in the noisy environments frontline workers often encounter.

To cope with noisy environments, background noise must be reduced to enhance the wanted audio signal. Minimising the mouth-to-microphone distance is a key factor.

Keeping your frontline staff safe is crucial. Make sure that your vendor can provide audio accessories with minimal mouth-to-microphone distance, namely those with an inline microphone.

KNOWLEDGE IS POWER

The first line of defense is always to provide knowledge and understanding about security threats among users of Bluetooth enabled devices. The increased awareness about security vulnerabilities should also be complemented by a centralised security policy and operational practices.

By combining the countermeasures with a robust security policy, frontline staff will benefit from secure, fast and always-on communications – keeping them safer and enabling them to perform at their best.

PUTTING IT INTO PRACTICE

Bluetooth has evolved markedly in recent years, making a unique contribution to how we use technology to keep public service personnel safe. Bluetooth devices benefit from significant security enhancements, but it's imperative to keep several steps ahead of threats such as eavesdropping, MITM and DoS attacks.

The five countermeasures that we've shared here don't require enormous efforts or investment; the degree of implementation should be based on the acceptable level of risk for your organisation. However, it's important to work with a vendor that has the technology in place to fully execute all the countermeasures, especially where the cost of a security breach is significant.

SOURCE

1. Bluetooth.org

The design of the latest MTP3000 and MTP6000 series TETRA radios from Motorola are informed by these countermeasures – ensuring that organisations can benefit from a mission-critical Bluetooth environment that is secure, fast and reliable. For further information visit **motorolasolutions.com/mtp6000**.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com**

MOTOROLA