RECOMMENDATIONS

TSCM, INFORMATION TECHNOLOGY (CYBER) & PHYSICAL SECURITY

Kindly note that for future TSCM tasks, we would appreciate it if a delegate from the Company's IT Department, who specialises in IT Security, accompany the TSCM Team. This is a preventative measure since the fields of TSCM and IT are closely related, and we need to point out possible concerns when it comes to server rooms/areas and server cabinets which are the responsibility of the IT Manager. Please refer to the following information in support of this request:

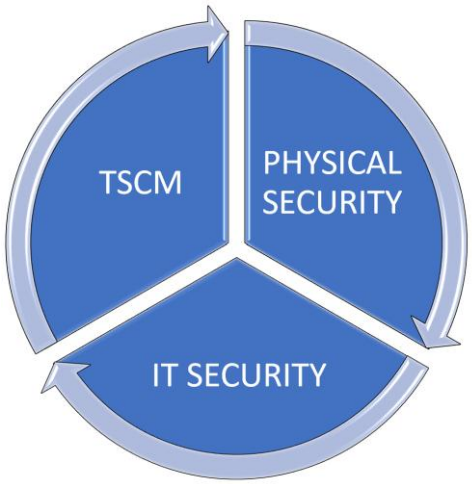

Figure 1: SECURITY TEAM COLLABORATION

a. TSCM (Technical Surveillance Countermeasures), IT (Information Technology) Security (Cyber Security), and Physical Security are three distinct fields that are indeed becoming closer in some respects, but important differences still exist because of their specific focuses and goals.

b. TSCM is primarily concerned with identifying and mitigating unauthorised surveillance or eavesdropping activities. This includes detecting hidden surveillance devices like electronic bugs, wiretaps, hidden cameras, and other electronic spying equipment. TSCM specialists use specialised equipment and techniques to perform physical inspections of spaces to ensure their integrity, confidentiality, and security.

   The goal of TSCM is to protect sensitive information, Intellectual Property, and conversations from being intercepted by unauthorised parties. This is done by doing a physical search of the room, interrogating the RF (Radio Frequency) spectrum looking for known carriers of voice and video or unusual carriers that stand out between the known RF carriers, and using electronic detecting equipment to scan inside objects in the room that can hide an electronic device, in a specific point in time.

c. IT, on the other hand, deals with the management, maintenance, and security of information systems, networks, software, and hardware. IT professionals work to **ensure that an organisation's digital infrastructure is functional, secure, and efficient**. They focus on tasks such as network administration, software development, cybersecurity, data management, and user support.

IT Security is a continuous process with constant monitoring of the infrastructure and data flows, from basic event logs that might be monitored real-time or periodically, to dedicated Intrusion Detection Systems, and Intrusion Prevention Systems, with well-known Anti-virus and complex passwords in the middle somewhere.

d. **Physical Security** is primarily concerned with the **protection of the premises, people, and equipment**. They are dependent on physical access control such as gates, doors, and locks, etc. Their main competency is their people, who can observe and based on experience, protect what needs to be protected. Physical Security is an exceptionally well designed and defined field, with a huge number of expert areas. The security manager is in most organisations also head of overall security that includes IT Security and TSCM tasks to ensure rooms are secure and private.

e. CONVERGENCE OF TSCM AND IT SECURITY (WORKING TOGETHER):

In recent years, there has been a growing convergence between TSCM and IT Security due to several factors:

- Digital Transformation: The increasing digitalisation of information and communication has led to more information being transmitted electronically, making it susceptible to interception. TSCM specialists are now required to have a better understanding of digital communication technologies to detect potential vulnerabilities.

- Cybersecurity Concerns: As the threat landscape has evolved, TSCM practitioners have recognised the importance of cybersecurity. Modern surveillance devices might be connected to networks, making not only the IT network susceptible to hacking, but also allowing eavesdropping devices using the IT infrastructure to send the recordings out of the site, bypassing traditional mechanisms. **TSCM PROFESSIONALS NEED TO COLLABORATE WITH IT EXPERTS TO ADDRESS THESE CYBERSECURITY RISKS**.

- IoT (Internet of Things): The proliferation of IoT devices has created new challenges for TSCM. Many of these devices are network-connected and could potentially be used for unauthorised surveillance. IT knowledge is necessary to understand and counter these threats effectively.

f. Despite these converging factors, **TSCM and IT still maintain key differences**:

Focus:

- TSCM is primarily concerned with physical space and electronic surveillance device detection.
- IT Security is broader and encompasses the entire digital infrastructure of an organisation.

Skill Sets:

- While there's some overlap, TSCM specialists need expertise in physical inspections, radio frequency analysis, and countermeasures specific to surveillance devices.
- IT professionals require skills in networking, software development, cybersecurity, and data management.

Goals:

- TSCM aims to prevent unauthorised access to conversations and information by detecting physical surveillance devices.
- IT aims to maintain the confidentiality, integrity, and availability of digital data and systems.

Training and Certification:

- TSCM specialists often undergo specialised training and certification specific to counter-surveillance techniques.
- IT professionals typically obtain certifications related to networking, cybersecurity, and software development.

g. WHY TSCM STAFF SHOULD NOT INTERFERE WITH IT SERVERS ON SCENE

- Expertise and Training: TSCM and IT professionals possess different skill sets and training. TSCM experts specialise in identifying covert surveillance devices, understanding the nuances of electronic signals, and employing countermeasures to ensure security. IT staff, on the other hand, have expertise in managing network infrastructure, software, hardware, and data management.

- Potential for Data Loss or Damage: TSCM staff may not fully comprehend the complexity of IT systems, databases, and applications. Attempting to make changes to servers, networks, and even Video Conference equipment, or configurations of these devices without the proper knowledge could result in data loss, system downtime, or even damage to critical IT infrastructure.

- Legal and Compliance Concerns: Unauthorised access or modifications to IT systems could potentially violate privacy regulations and laws, such as data protection acts. IT personnel typically follow protocols to ensure compliance with legal requirements, whereas TSCM staff may not be well-versed in these regulations.

h. TSCM versus IT SECURITY

- Disruption to Operations: Interfering with IT servers or networks without proper authorisation and understanding could lead to disruptions in business operations.

IT systems are often integral to the day-to-day functioning of an organisation, and any tampering could lead to downtime or loss of productivity.

- Miscommunication and Confusion: Organisations often have established protocols for addressing IT-related issues. If TSCM staff intervene without proper coordination and communication, it can create confusion and misalignment between different departments.

- Lack of Accountability: If TSCM staff make changes to IT systems and something goes wrong, it might be difficult to assign accountability. IT personnel are trained to manage and troubleshoot issues related to the technology infrastructure and can be held responsible for their actions.

- Specialised Tools and Equipment: TSCM experts use specialised tools and equipment designed for detecting and neutralising electronic surveillance devices. **These tools are not intended for IT system management and could cause unintended consequences if applied to IT servers**. See TSCM equipment and functionality on www.acsolutions.co.za.

- **Collaboration and Communication: In cases where TSCM concerns intersect with IT systems, collaboration, and effective communication between TSCM and IT teams are essential. The two teams can work together to address security vulnerabilities without compromising IT infrastructure.**

i. In situations where TSCM staff believe that electronic eavesdropping devices are affecting IT systems or networks, the best approach is to collaborate with the IT department to ensure a coordinated response. Open communication and clear delineation of roles and responsibilities can help avoid misunderstandings and negative outcomes.

j. **The increasing digitalisation of information and communication has brought TSCM and IT closer together, necessitating collaboration to address new security challenges. However, their distinct focuses, skill sets, and goals mean that they will continue to remain separate but interconnected fields.**

k. The identification of IT equipment, i.e., Pocket Port, Keyloggers, Rubber Duck and other similar equipment could be hidden or disguised in various forms and sometimes difficult to identify without proper IT knowledge. It is often hidden in plain sight and will look to most IT and TSCM professionals when viewed on their own, like a normal IT device. **When the teams work together to understand why the device might be there, they can share the analysis and identify the possible threat**, and either analyse the device there and then, or remove it from the environment to analyse it in a secure environment without compromising the IT systems' integrity.

RECOMMENDATIONS

TELEPHONES AND NETWORK SECURITY

It is suggested that all Analogue telephones (fax lines) and other lines involved be replaced with **ISDN/VoIP lines (Digital).** This specific type of communication line enables greater communication security. **Please take note of the following information and recommendations on Internet, VoIP, and Wi-Fi technology.**

a. **Voice over IP (VoIP, or voice over Internet Protocol**) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone.

b. A major development that started in 2004 was the introduction of mass-market VoIP services using existing broadband Internet access, by which subscribers place/receive telephone calls in much the same manner as they would via the public switched telephone network (PSTN). Full-service VoIP phone companies provide inbound and outbound service with Direct Inbound Dialing. Many offers unlimited domestic calling for a flat monthly subscription fee.

c. Dedicated VoIP phones connect directly to the IP network using technologies such as wired Ethernet or wireless Wi-Fi. They are typically designed in the style of traditional digital business telephones.

d. Irrespective of which technology your company uses, all these systems are vulnerable and vulnerable via the latest software tools which enable theft of data as easy as browsing the web. Currently very few network security products are available in the market that can understand both the working and functionality of VoIP devices and VoIP technology, and which can provide added security features to ensure secure communication between two or more VoIP communication channels.

e. Telephones have microphones, speakers, ringers, microphonic transducers, and power all of which can provide everything an eavesdropper needs to listen in on corporate / business or personal affairs. We employed the following state of the art equipment and technology to assess the VoIP technology during our TSCM task:

- **TALAN DPA 3.0 Telephone & Line Analyser (VoIP Analysis / VoIP Traffic Analysis)**

Voice over IP (VoIP) technology encodes speech for transmission over IP (internet protocol) networks. TALAN has the ability to monitor IP packet traffic using its built-in network interface card (NIC) and to display, analyse and save those packets to assess the threat of illicit VoIP phone system intrusions.

- BLOODHOUND Shearwater 2000 (Identification of Microphone Modification/Tampering)

Bloodhound is an ASMD, Acoustically Stimulated Microphone Detector which is an electronic system for use by Technical Security Inspection Teams for detecting audio eavesdropping. The system works by detecting the radiated field created whenever a microphone detects sound. The Bloodhound operator can either listen to the detected audio or establish acoustic feedback.

Inside the telephone is a switch that disconnects and shorts out the microphone in your telephone handset when the telephone is hung up (hookswitch). If the telephone circuitry is slightly modified the microphone will be "hot" all the time. If the microphone is “hot” all the time, then the eavesdropper can go anywhere outside that area; plug an audio amplifier into the phone line; and get excellent quality room audio. It is effectively the same as installing a microphone or eavesdropping device in the room or building (no actual “bug” is used).

Off Hook - Used to denote the state of a telephone during an active call, or when a call has been initiated. For a handset phone, off hook usually means that the handset is lifted.

On Hook - Used to denote a telephone in the idle state – no call started or answered. A telephone is still on hook when it is ringing on an incoming call. For a handset phone, on hook usually means the handset is not lifted.

f. We recommend that your Company secure itself against employees or hackers conducting attacks with malicious intent, including, and not limited to malicious software such as Spyware, Key Loggers (keystroke capturing), Phishing, Viruses, Worms, and Trojan Horses which attack Company Servers and Cyber Security.

g. We may also assist in the identification of the correct Company to provide Forensic Assessments and “in-house” development of Security Products, not known to Hackers and Employees, able to successfully identify and prevent such attacks.

h. Additionally, the provider could successfully retrieve lost or corrupted data from Servers, Workstations, Laptops, Computers, Computer media and more recently from Cell Phones. This specific IT Security, and Digital Forensic expertise, can provide a more secure and comprehensive customised solution, either to be used over the Internet or within a Local Intranet Environment to ensure VoIP Communication Security.

MOBILE DEVICE SECURITY

Mobile devices, including smartphones and tablet computers, offer enhanced functionality and ease of use to users anytime, anywhere. Smartphones have become the new personal computers, housing vast amounts of both personal and business data. As technological advancements continue to accelerate, our daily lives are increasingly reliant on these wireless devices, which, unfortunately, also expose users to heightened risks and unique security threats.

Mobile device malware (malicious code) has surged in recent years. The sophistication of these threats has grown exponentially, making detection and removal significantly more challenging. In fact, anyone with access to your smartphone, even for just a few minutes, could install eavesdropping software. This software can grant them access to sensitive data, such as SMS messages, emails, photos, location information, call logs, and even live phone calls.

Certain types of malicious code can also enable attackers to remotely activate the device's microphone, allowing them to listen in on conversations, or turn on the camera to take photos without the user's knowledge.

For more information, please click here.

Our partner company, **Dynamdre**, specialises in mobile device investigations to retrieve data from devices that may be infected with malicious software.

Visit www.dynamdre.co.za and contact **Dynamdre** directly for further assistance and inquiries.

WI-FI SECURITY

In response to the COVID-19 pandemic, many companies swiftly adopted "work-from-home" policies. While these changes were essential, they had an adverse impact on organisations by altering the way we work and introducing new information security risks. During these challenging times, cybercriminals have made it clear that they are not slowing down. In fact, we have observed a significant increase in cyberattacks in recent months.

As "working from home" becomes the new norm, it brings with it substantial security risks. Many companies, along with their ICT teams, were forced to quickly implement remote working tools and services, often relying on insecure connections that were not fully vetted for security.

A recent survey of 300 remote workers and 300 ICT professionals highlighted several concerns. For example, 57% of remote workers rely on communication tools such as Zoom and Microsoft Teams, which have recently faced well-documented security vulnerabilities.

Risky cybersecurity practices were especially prevalent among working parents, who often face additional distractions such as childcare and homeschooling. Within this group, 57% reported saving passwords insecurely in their browsers on corporate devices, while 89% admitted to reusing passwords across multiple applications and devices. Furthermore, 21% allowed other members of their household to use corporate devices for non-work activities such as schoolwork, gaming, and shopping. Despite the rising security risks associated with remote work, 57% of ICT professionals surveyed indicated that they have not increased security protocols during this period.

It is a well-established fact that home networks, and specifically home Wi-Fi networks, are far less secure than corporate networks, which presents another significant risk to businesses. In many cases, once a wireless router is installed, it’s placed in a corner and largely forgotten. As long as all devices are connected to the Wi-Fi network, many assume it’s secure. However, this assumption is often misplaced.

In reality, the internet router is one of the most critical devices in our homes. It serves as the gateway to our internet access and is a prime target for cybercriminals. If compromised, it could give attackers access to all devices connected to the network. In today's environment of data breaches, ransomware attacks, and other online threats, securing the home network should be a top priority.

To address these concerns, **Dynamdre**, in collaboration with **Advanced Corporate Solutions (ACS)**, offers formal Wi-Fi security assessments for residential environments owned by executives of various organisations. These assessments provide insights into the resilience of executives' home information security posture, evaluating both their ability to withstand unauthorised attacks and the potential for authorised users to abuse their privileges.

Key Technical Controls and Security Assessment Areas include, but are not limited to:

- Identification of Rogue Wi-Fi Access Points
- Default Credentials (Router-Based Access and Wi-Fi Passkeys)
- Unencrypted Wi-Fi Networks
- Legacy or Weak Encryption
- Outdated Router Firmware Versions
- Network Segmentation
- DHCP Functionality Check
- Wi-Fi Passkey Strength Test
- Residential Wi-Fi Vulnerability Assessment