HIGHPOINT SECURITY TECHNOLOGIES Inc.

Beyond TSCM : Policy, Procedures and Employee Awareness

James Phillips
Manager Technical Security
416 840 4919
james@hipoint.ca

TSCM

Technical Surveillance Countermeasures

- Security Inspection & Consultation to identify and mitigate threats of electronic and covert interception.
- Conducted by experts in the field.
- Uncover immediate threats

TSCM

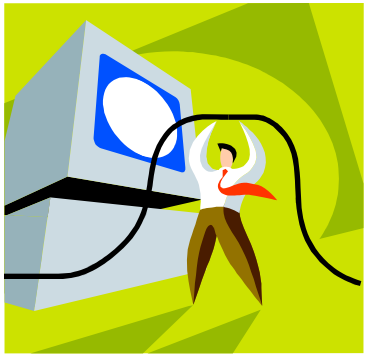
A Technical Security Inspection is a "***Point In Time***" test.

This means: the TSCM expert can indicate that at this particular point in time your environment is clear of electronic devices.

What happens when they leave and you are not prepared?

TSCM

You are ***VULNERABLE*** to new attacks.



TSCM

The field of Technical Inspections has 2 main limiting factors for most companies to practically consider performing “in house” and on a day to day basis:

- Expertise to interpret results properly
- Cost of equipment

TSCM

It is for these 2 main reasons that businesses need to take a serious look at their policies, procedures and employee awareness. By being ***PROACTIVE*** this will help ensure the confidentiality of sensitive company information.

A New Look

We are probably all very familiar with policies, procedures and employee awareness. However, we can also sometimes forget to look at these through our many perspectives.

Beyond TSCM

Purpose:

The purpose of today's presentation is to look at the various policies, procedures and employee awareness programs with a Technical Security (electronic/covert espionage) perspective.

Policy

Back to Basics:

A ***policy*** is a plan of action to guide decisions and actions.

Source: www.wikipedia.org as of April 19, 2006

Policy

Do you know what policies you have that can be modified to include the TSCM perspective ?

Think like a TSCM professional and do not under estimate ANY threat.

Policy

Do you have a Acceptable Use Policy for your computer workstations and company technical hardware?

Do any of the computers at your company look like the one on the next page?


SECRET COMPANY FILES
NO SCREEN SAVER PASSWORD!!
RADIO'S
THOMSON
21 10:15AM


21 10:15AM

Policy

This scene is quite popular these days due to the technological devices available to consumers.

- Make sure you make the distinction between which devices are ABSOLUTELY necessary for company work and which are prohibited.

Policy

Think about how technology has changed and how this change in technology could perhaps influence our perspective.

- Think back even only 10 years ago - if you would see an employee walking around with a mini tape recorder this may have been viewed as suspicious activity.

- Move ahead 10 years – I do not think anyone would consider an employee walking around with a digital recording device (Ipod) as suspicious even though this device presents considerably more of a threat than a tape recorder. The digital recording devices have : much larger capacity, capabilities to record pictures-sound-data files, much longer battery life, smaller in size and easy to conceal.

Policy

Considerations from the TSCM Perspective:

Technological Devices

- Do not allow employee's to connect devices such as personal cameras, digital storage devices (mp3 player, flash drives, Ipod's), bluetooth headsets, web cameras.
- If employee job function does not need USB devices -> disable them.

Hardware

- Do not allow authorization for employee's to open or modify company hardware. Use security screws or tamper tape to prevent this.
- Restrict access to hub/switch rooms, floor plates, ceiling tiles

Data Safe Guarding

- Ensure confidential material is stored in a secure location on the server.
- Screen Saver Password
- Clean Work Environment
- Storage of Passwords (not on post it note)

Policy

- Manage the policy.
- Enforce the police (employee awareness)
- Update policy as technology changes
- Review Policy – use many perspectives when reviewing
- Do not refer to a policy when you need it. Treat the policy like the proactive day to day measure it should be!

Good Policy

Use your policy to make sure the employee's know what is considered sensitive, confidential and secret information.

- Use you policy to help guide your employee's to make the right decisions.


21 10:20AM


21 10:20AM

Procedures

Procedures outline in a step by step fashion how you do something.

You should view procedures as the “how you do something” in a policy.

Procedures

Procedures are very important because they help assist the employee to adhere to policy.

- Procedures are ***PROACTIVE*** measures.

- Chances are if you are not using procedures, you are familiar with investigations. Investigations are reactive activities which means something out of policy has occurred.

Procedures

A view from the TSCM Perspective

Pre Meeting Procedures

There are usually more rules and procedures around who gets to use the boardroom and when they get to use it then how to secure it !

- When booking a boardroom the questions to ask are?
- What is the security level of your meeting?
- Is a professional sweep required?
- Is the host of the meeting trained in conducting basic physical inspection?
- Have you notified corporate security of your meeting?
- Do you have a list of all attendees including, name phone number, address?

Post Meeting Procedures

Have you ever seen the state of a boardroom at the conclusion of a meeting?

Who is responsible for a post meeting physical inspection?

Courier/Visitor Procedures

Do you allow your courier or visitors unescorted access to parts of your building? (beyond reception, kitchenette, receiving)

- Now before you say no -> go and watch the front reception or receiving for a few hours and then answer.

Plan Ahead Procedures

Visitors should always be booked ahead of time with reception. The visitor should be met at the door by the host and then escorted to the meeting room (never a cubicle). If in an office, never leave visitor alone (have coffee brought to you).

Procedures

Do you currently have procedures to help protect the confidentiality of your information?

- If yes -> are they effective? Do you test them?

Considerations

- Contractor Log Book (in each boardroom)
- Reception Log Book
- Document / Data destruction
- Reporting suspicious activity
- Conducting off site meetings
- Environment Physical Scan

Employee Awareness

Employee Awareness is the act of educating and reinforcing of policy & procedures to increase compliance.

We can not expect people to make all the right decisions all the time. It is important to keep reinforcing topics to drive them to become automatic actions.

Employee Awareness

- Teach ALL employee's the nature of electronic and covert espionage.

We live in a fairly trusting society where things like security, electronic espionage, industrial spying are not on everyone's mind.

- Most people have only ever seen this stuff on TV. Show them real equipment with real facts.

Employee Awareness

In many cases, employee's do not comply because they feel their job is not significant enough to be a factor.

- You need to show them how their own contribution to security and reporting suspicious activity can ***SIGNIFICANTLY*** reduce the risk from a threat.

Employee Awareness

- Teach employee's how to conduct their own environment scan to identify suspicious devices.
- The employee does not even have to know what a bug looks like. They just need to learn how to identify when something has been added or changed in their environment.
- Create a procedure for a weekly environment scan of ALL employee's workspace.

Employee Awareness

Employee's can be the weakest or the strongest link in the chain. It really depends on their compliance.

As security professionals, we know how to design secure networks, secure structures, we design policy, we write procedures, we implement state of the art technology.

- However -> it only takes 1 employee to not follow procedure to undermine ALL of that work.

Employee Awareness

Educate Through Proper Training Sessions

- Allow employee's the time to attend and make them feel a sense of ownership. Have them sign in to the training. Make it interactive and relevant to them.
- Invite TSCM professionals to come in and talk about the business.

Employee Awareness

Reinforce Awareness

- Never use employee awareness to threaten or discipline employee's. Make sure they understand it is important to review the topics and to monitor the success of the training. If procedures are not being followed this is a good starting point to find out from the employee's why? Can the procedure be changed to make it easier to follow?

Employee Awareness Off Site

Discuss with employee's the importance of maintaining confidentiality while traveling.

- All employee's are potential targets.

Traveling Considerations

- Laptop / Briefcase storage
- Places not to talk or work – coffee shops, planes, trains, buses or any of the above stations.
- Prepare for travel. Remove sensitive information from laptop or briefcase. Maybe have a second laptop just for traveling.

PEP Talk

Introduce your employee's to the PEP talk.

People

Environment

Places

PEP Talk

- The PEP talk is a simple solution to help your employee's maintain confidentiality while on the road.
- Employee's should be taught to run through each of the letters in PEP before discussing ANY company information.

People

- Who are the people I am meeting with
- What is the security level of the information we are going to speak about?
- How much trust do I place upon this person? Are they recording this conversation?

Environment

- Is this a suitable place to discuss business ?

- Who else can over hear what we are discussing ?(waiters, cab drivers, public walking by)

Places

- Are there places where devices could be hidden to listen us? (plants, bushes, fake clock)
- Are there places where people could over hear us? (back to back benches, restaurant booths separated by flowers or curtain)

- Am I in a situation where someone could reasonably be standing beside me without being suspicious of them? (bank of telephones- how would you know if they are really on the phone?)

PEP Talk

The PEP talk is not designed to have all the answers. It is designed to make the employee think about their situation and make the best decision based on the available information.

- I have heard from employee's- I didn't even think the guy beside me at the telephones would take my briefcase…

In Conclusion

This presentation has been prepared to help us think with a TSCM perspective. All environments are different and will require different approaches.

- The best approach in security is to layer your security.

Putting it all together

Professional Security Inspection

Good Policies

Good Procedures

Training and Reinforcement

Monitor –policy infractions / suspicious activity

Report – infractions / suspicious activity

Review Effectiveness

Professional Security Inspection

Opportunity

- All approaches should be designed to remove or lessen the availability of ***OPPORTUNITY.***
- If the opportunity is available it can and will most likely be exploited at some point in time.
- If you take away the opportunity, you have also taken away a number of potential threats.