
# Simple strategies to make your business more secure

**How to stop the bad guys from stealing your stuff without you noticing**

# What motivates the bad guys

## Crime in general

One on one

One on Many

One on Millions

Money, access to money

Intellectual Property / Trade secrets

Client, staff and business information

Your technology

## The basics have not changed

Motive

Means


Opportunity

# If you think security is…

It will never happen to us

You have a problem!


You have a problem!

My IT / Managed service provider has that covered

You have a problem!

We have nothing of value

You have a problem!

You are too small to be a target

You have a problem!

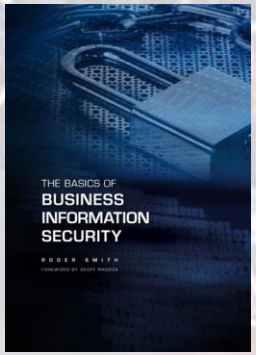
We take security seriously but have not invested in security

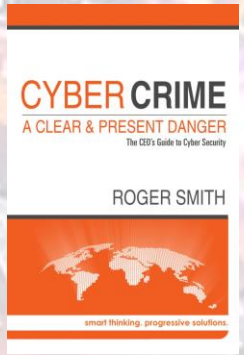
# Why US

## Work experience

- In the ICT industry since 1984
- Run my own business in the security space since 2011
- Teach at Australian Defence Force College
- Teach at CIT

## Author





## Achievements




## Education

Numerous Vendor and industry certification.
Our competition do not have certs

## Contact Info

**Roger Smith**
**02 62577792**
**https://caremit.com.au**
**Roger.smith@caremit.com.au**

23 AUGUST 2022

# Insider Threat & Workforce Assurance

INSIDER THREAT

## Defence Teaming Centre

Presenter: **Tim Slattery**
**Senior Director**
**Enterprise Protective Security**

Providence

# Today - Digital Crime is a business!

**THERE is**

**Competition and collaboration between rival gangs**

**Web Hosting, Botnets, Zombie networks, Malware and exploit kits, money laundering, crypto exchanges**

**Operations and Automation**

**Research and Development**

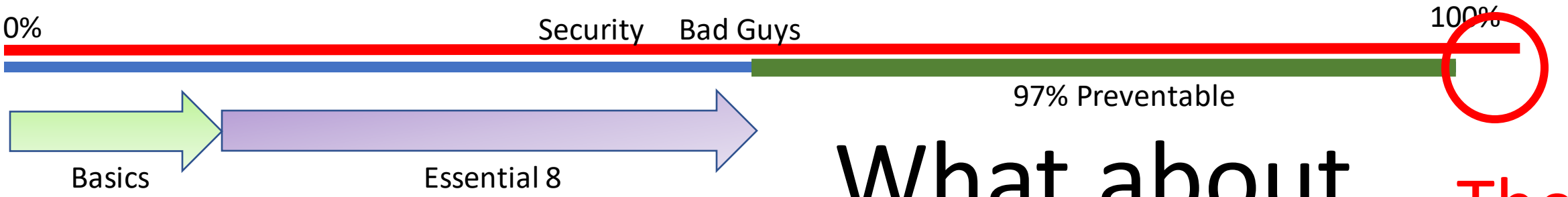
**Marketing and Sales**

**Support**

**Random Vs Targeted**


**The cybercriminal space is Darwinian – the bad get caught, the good get better! (we have to stop the good)**

# Why we should be concerned with protecting ourselves and our systems




What about this 47%

The missing 3%

**Protecting against the 47%, we call that enhanced business security**

# What you need to know to protect your organisation

**What are your assets (people, information, property, reputation).**
**What are the risks to them and how do you mitigate them?**

## Stop them getting in

**Are you seeing what the cybercriminal see from outside your environment - (continuous vulnerability scanning, penetration testing, dark web scanning, social media scraping)**

# Insider Threat: Definition

- The potential for an individual who has, or had, authorised access to an organisation's assets to use those assets, either maliciously or unintentionally, to act in a way that could negatively affect the organisation.
- Usually associated with cyber security

*National Insider Threat Centre (NITC), Carnegie Mellon University*

# Data on Insider Threat

- Pandemic has increased the insider threat:
  - 278 organisations
    - 6803 insider incidents (56% - negligent, 26% - malicious, 18% - credential theft)
  - 44% increase of insider-led security incidents in 2022 (comparison to 2020)
  - $15.4M - total average annual cost of insider incidents ($11.45M in 2020)
  - Containment of an insider threat incident rising from 77 days in 2020 to 85 in 2022.

*2022 Cost of Insider Threats Global Report (Ponemon Institute)*

# Why is Insider Threat relevant to you?

- You may have one now.
- You may have more than one now.
- You may recruit one soon.
- How might you know the risks in your current or future workforce?

# Workforce assurance standards in Australia

**Australian Standard for the Workforce Screening (AS 4811:2022)**

**Protective Security Policy Framework: Adjudicative Guidelines**

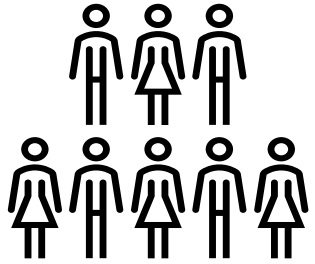
**7 key risk factor areas:**

- External loyalties
- Personal relationships and conduct
- Finance
- Use of alcohol and drugs
- Criminal history and conduct
- Attitude to security / security violations
- Mental health disorders

**... and what nominated and unnominated referees say about you**

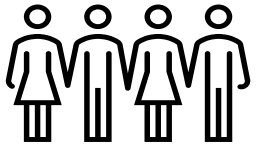
# Available screening options

| Type of a personnel security check/ assessment | **AGSVA baseline security clearance** | **AusCheck background check (Home Affairs)** | **Private company background checking** | **Providence Workforce Assurance Model …** |
|---|---|---|---|---|
| **Availability for the private sector** | ✓ Limited<br># sponsored by the Australian Government | ✓ Critical infrastructure<br># (limited by legislation) | ✓ Yes | ✓ Yes |
| **AS 4811:2022** | ✓ Old standard | ✓ No | ✓ Old standard | ✓ Yes |
| **PSPF** | ✓ Yes | ✓ No (only 2 risk factors) | ✓ No (limited risk factors) | ✓ Yes |
| **Legislative base** | ✓ No | ✓ Yes | ✓ Yes (contract) | ✓ Yes (contract) |
| **Validity** | ✓ 15 years | ✓ 2 years | ✓ Point-in-time | ✓ Ongoing |
| **Timeframes** | ✓ 12 weeks + | ✓ 6 weeks + | ✓ 10 days + | ✓ Scalable (in house) |
| **Cost** | ✓ $884 | ✓ $100 | ✓ $210.20 | ✓ Scalable |



LOW

EMPLOYEE RISK CONTINUUM



HIGH

MULTIDISCIPLINARY GROUP

WORKFORCE ASSURANCE MODEL (CULTURE)

ACCESS AND TECHNICAL CONTROLS

MONITORING

DATA ANALYSIS & REPORTING

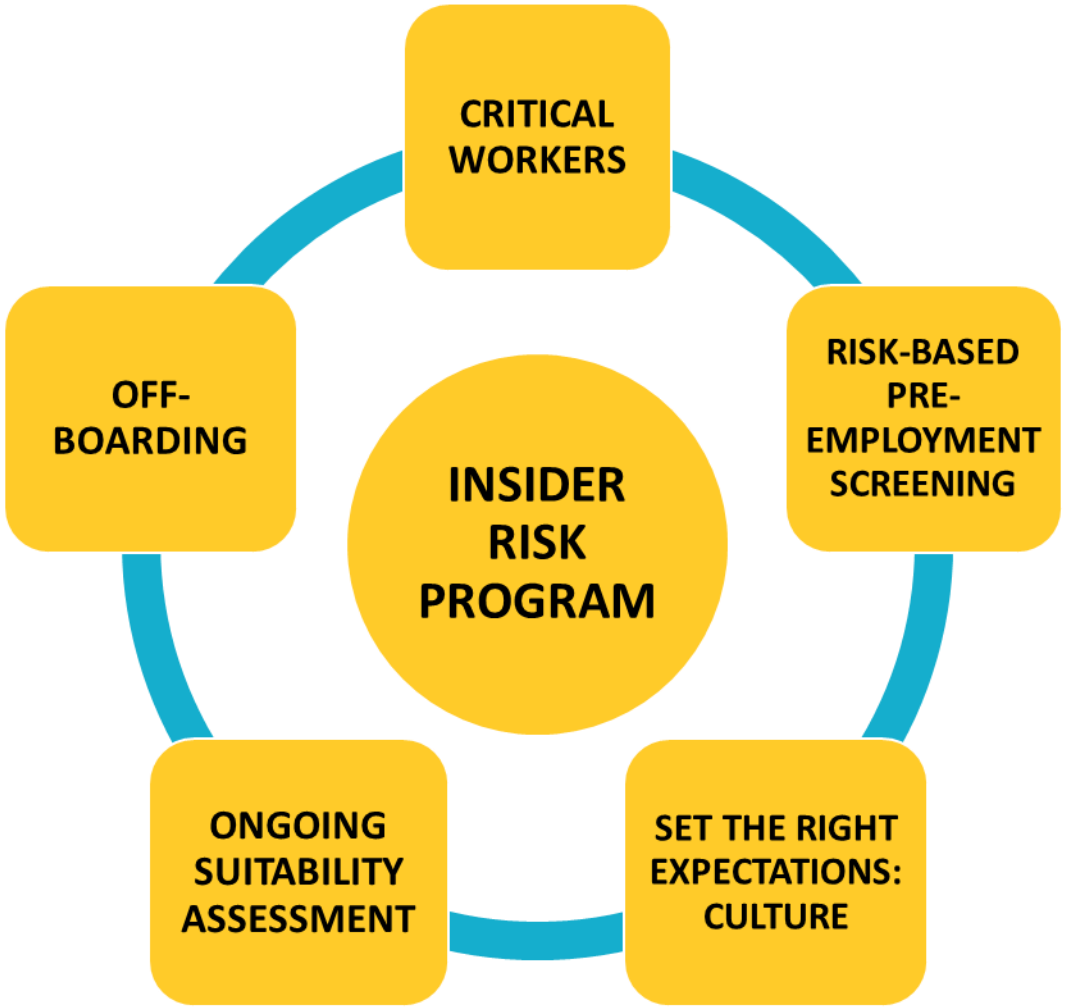
MONITORING

# INSIDER THREAT PROGRAM FOUNDATION

# Return on Investment: Insider Threat Program

- Holistic and risk based, in-house
- Shared responsibility within organisation
- Integrated protection of critical assets
- Early detection capability, minimising impact
- Adequate organisational response minimising threat
- Enhance organisation's security culture
- Bolster wellbeing, performance & diversity

# SOCI PERSONNEL SECURITY REQUIREMENTS



# What you need to know to protect your organisation

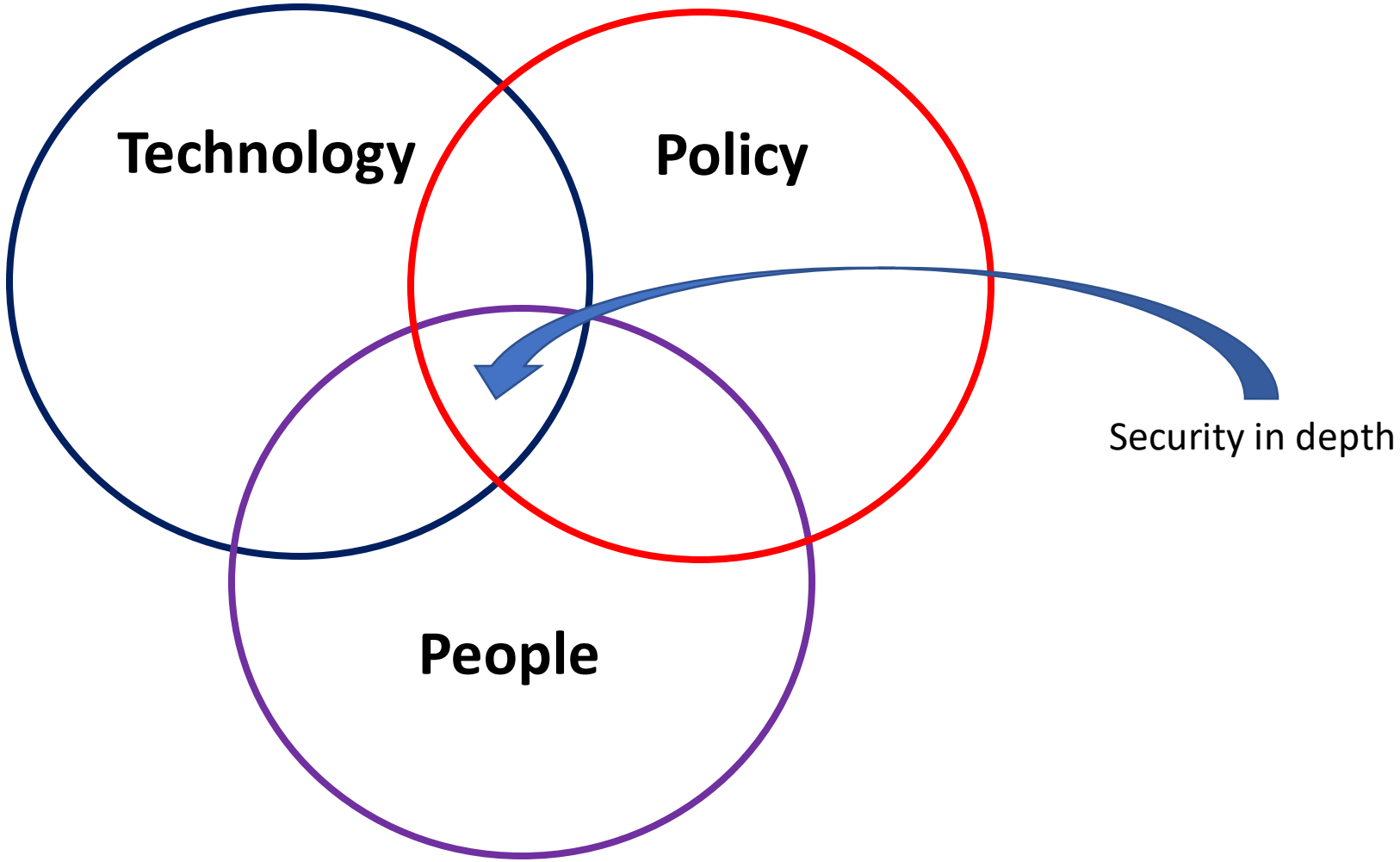

## Know what they have done

**What can you see inside your environment (System information and event management - SIEM, Reports, alerts, visuals)**

## Can you recover

**How can you get back to business as normal with minimal down time?**

# The basic building blocks of business security



# Why this is important?

**There is no “set and forget” when it comes to security**

**If we do not know who they are, how do we protect against them?**

**If we do not know what needs to be secure, how do we stop them?**

**If we do not do the basics, we cannot build better security?**

**If we are not proactive, how do we anticipate them?**

**If you do not start, how can you protect your business.**

**Your people can be your worst enemy or your best defence.**

**The insider threat needs to be addressed**

**Awareness, training and education is the key**