tesserent
Cyber Solutions by Thales

Cyber Security Awareness and Risk Mitigation

Andrew Shea, Managing Partner – Tesserent Academy
Linda Li, Head of Partnerships – Tesserent Academy

Andrew Shea
Managing Partner

Linda Li
Head of Partnerships

tesserent
Cyber Solutions by Thales

We offer Cyber 360 Services

Tesserent offers a comprehensive suite of cybersecurity services, technology and highly qualified and experienced consultants.

Incident Response

Advisory & Strategy

Tesserent Academy

Security Architecture & Engineering and Data Analytics

Managed IT/Cloud services

Critical Product Controls

Offensive Security

24/7 Security Operations (SOC)

tesserent
Cyber Solutions by Thales

Why Cyber Security

1

DEFINING CYBERSECURITY

Confidentiality

Information is only disclosed to authorised users

Integrity

Information is only **created**, **modified**, **destroyed** by authorised users

Availability

Information may be **reliably accessed** within **given timeframes**

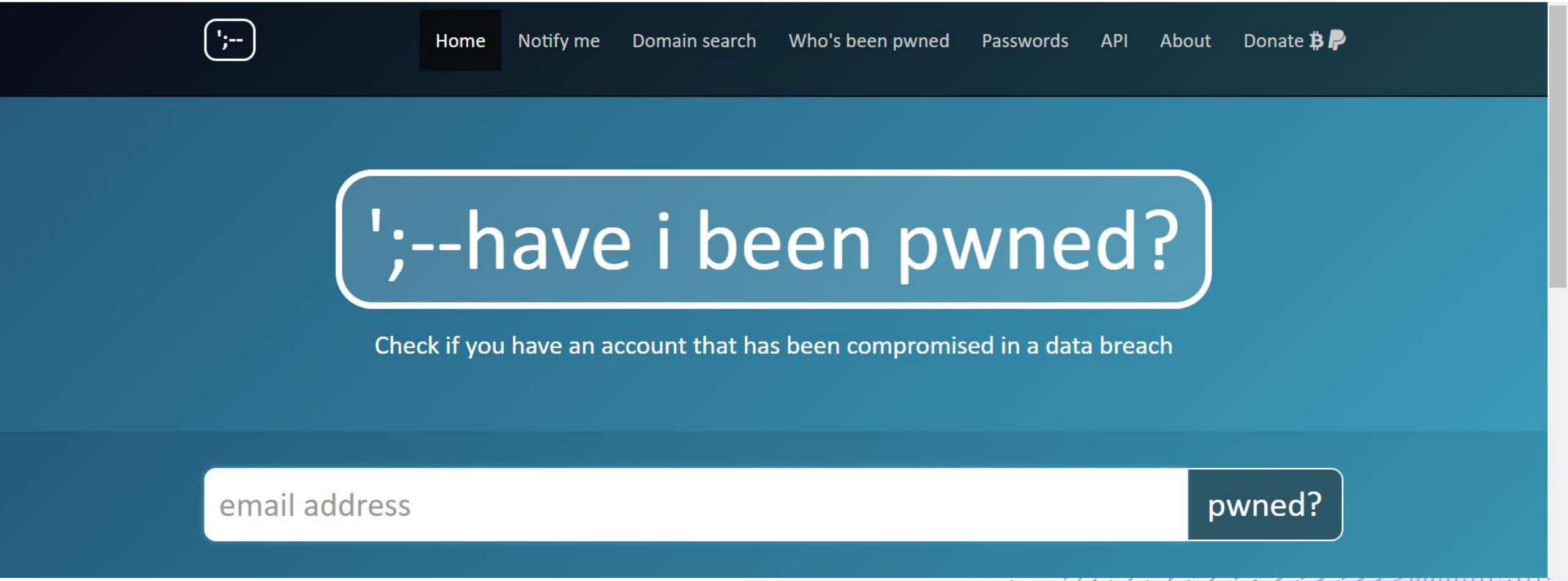
CYBER SECURITY AWARENESS

As responsible digital citizens, we need to build good habits in both our personal and professional life.

Responsible social media usage

Responsible password management

Defend against phishing attacks

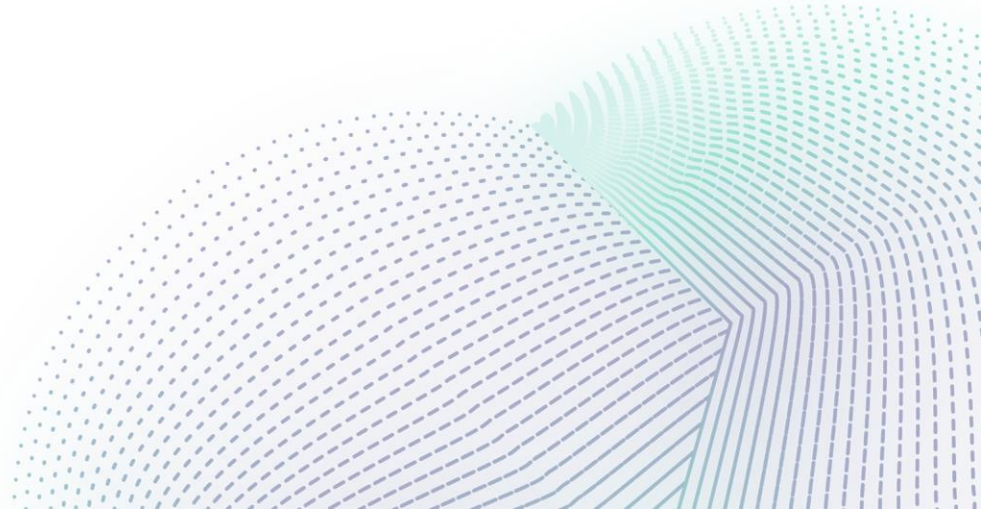

https://haveibeenpwned.com
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?

Threat Landscape

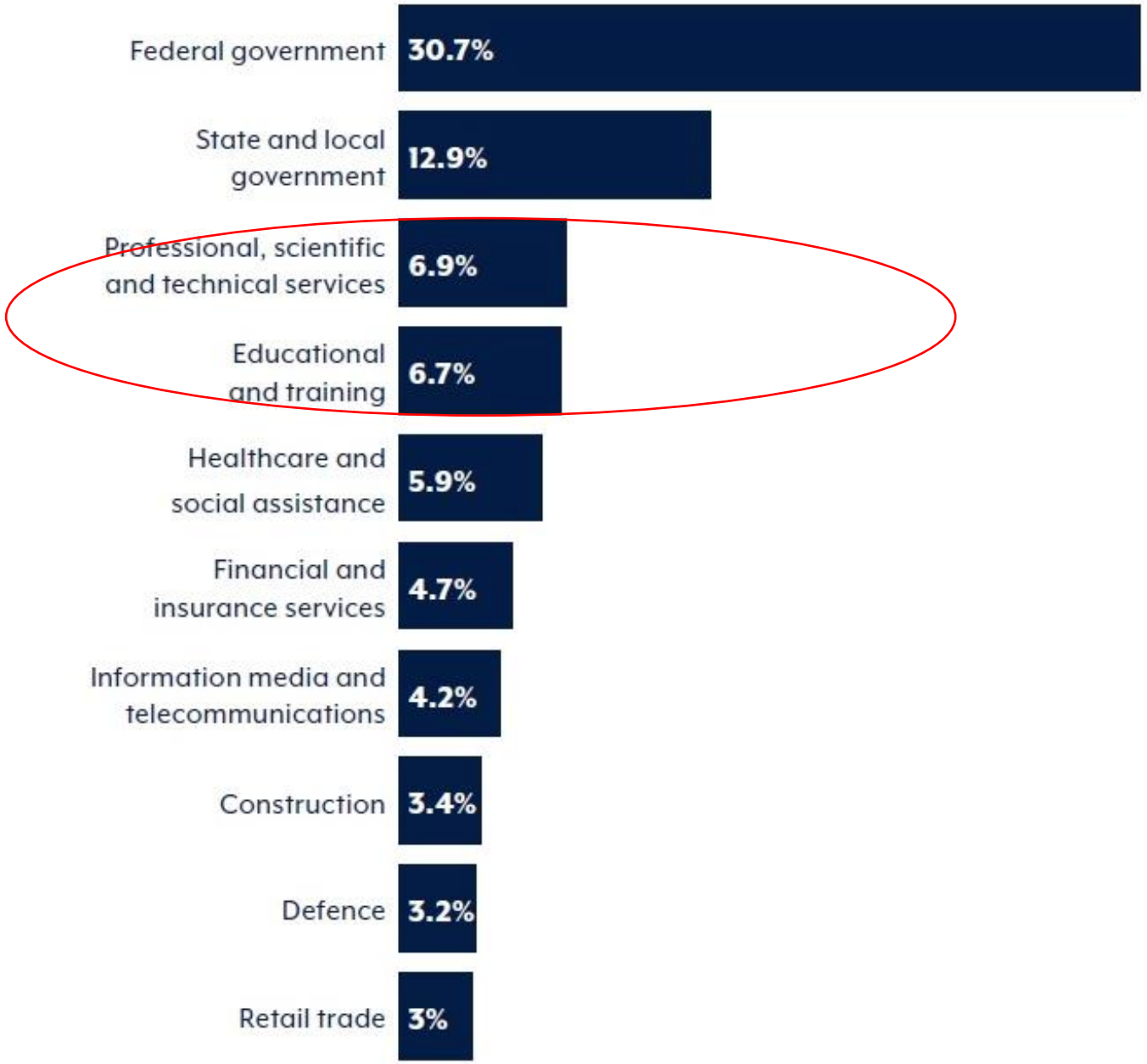
2

There are two kinds of companies; those that have been hacked, and those that have been hacked but don't know it yet.

U.S. House Intelligence Committee Chairman, Mike Rogers



cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023



Threats to your Assets

Attack can be opportunistic, likelihood might be low, but impact, if not properly prepared for, will still be high. As a business, this needs to be decided in collaboration with various stakeholders and properly communicated across the organisation to ensure the right threats are measured accordingly to the risk appetite of the business.

Loss of Data

Supply Chain Attack

Financial Fraud

Risk Management

2

One of the main cyber-risks is to think they don't exist.
The other is to try to treat all potential risks.

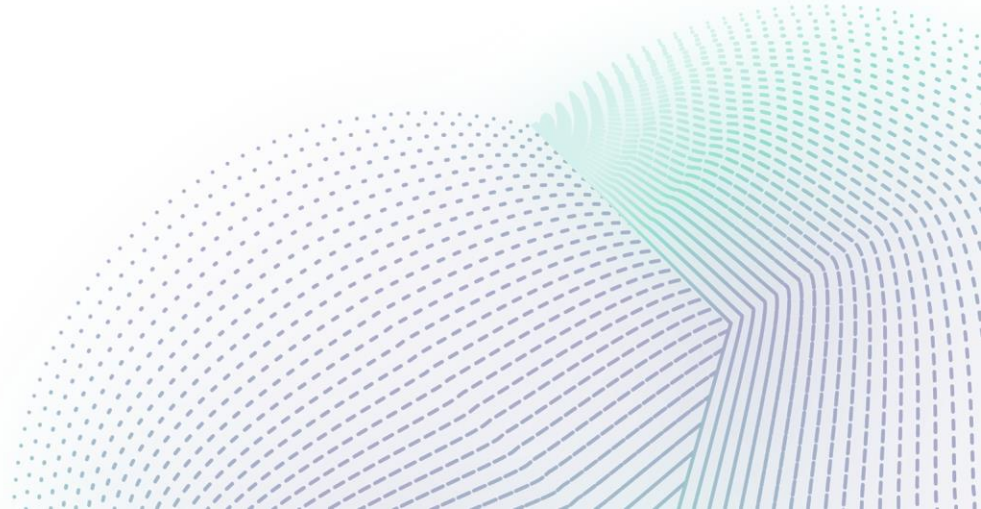
Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation.

Stéphane Nappo, Chief Information Security Officer of the Year, 2018

Risk Management

Risk Management is all about **professional judgement** and exercising **due diligence**:

- Balancing the likelihood of threats materialising with potential business impact
- Ensuring controls have been implemented and are working **efficiently** and **effectively**
- Ensuring continuous improvement over risk management practices
- Rate cyber risk as any other enterprise risk



Risk Management - Common Standards & Frameworks

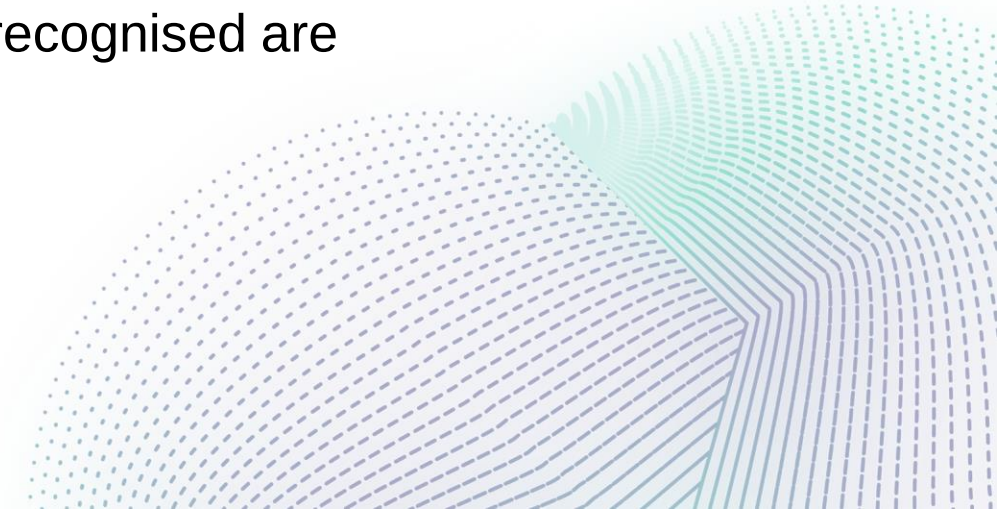
Many frameworks start with the identification of an organisation's assets, followed by a risk assessment coupled with the key control objectives relevant for an organisation's needs. These control objectives are often based on strategic requirements, and tailored to achieve the desired outcomes of the organisation.

As the organisation evolves, additional controls may be required to comply with changing conditions, new regulations, and contractual obligations.

Along with Australia's own ASD defined - **Essential Eight**

Common frameworks used in Australia that is internationally recognised are

- **ISO/IEC 27001**
- **NIST Cybersecurity Framework**



Right Fit for Risk

This accreditation process is applicable to:

- Employment Services Providers
- Australian Apprenticeships Support Network Providers
- Certain Skills program Providers and
- Third Party Employment and Skills systems (TPES) vendors.

Category One:
Providers and Subcontractors delivering Services to 2,000 or more individuals per annum because of all their Deeds. Third Party Employment and Skills (TPES) System vendors obtaining accreditation are also classified as Category one.

Category Two:
Providers and Subcontractors delivering Services to fewer than 2,000 individuals per annum because of all their Deeds. This category includes two sub-categories referred to as “Category 2A” and “Category 2B”

Category 1 Providers

- ISO27001 independently certified
- Annual surveillance audit and triennial recertification

Category 2A Providers

- ISO27001 conforming
- Annual self-assessment

Category 2B Providers

- Management Assertion Letter
- Annual Management Assertion Letter

RFFR Core Expectation: Cyber Security

- The Essential Eight
- Information Security Risk Management
- Information Security Monitoring
- Managing cyber security incidents
- Restricted access controls

Right Fit for Risk - Approach

- **ISO27001 certification or alignment**
  - Plan – Do – Check
  - Limiting your ISO27001 scope
  - Aligning to business risk and business priority
- **Invest in training – ISO27001 Lead Implementer and Lead Auditor Course.**
  - Risk and Compliance professionals are perfect for ISO27001 training
  - Upskilling is the best way to retain staff
- **In-house vs Outsourced**
  - Ultimately accountable, ensure you still understand the risks.
  - Third party assessment

Key Take Aways

- Promoting a strong cyber awareness culture
- Ensure strong password management – don’t share accounts!
- Minimise access control across systems – access for only those that need it.
- Multi-factor authentication turned on across all log in.
- Ensure the latest version of all systems and applications are being used.
- Are you using third party SaaS solutions? – have you asked them for their most recent pen test or ISO accreditation or similar?
- Who’s responsible for risk and compliance, do they understand ISO27001? What kind of training have they done?
- Do you have back up set up. Have you tested this> do you know how quickly it can be restored? and is the frequency of back up supportive of the data value?

Thank you.
Look forward to connecting.

Linda.Li@tesserent.com
0408140283

Book a meeting:

SCAN ME

Connect with me on LinkedIn

SCAN ME