Understanding the Insider Threat, and Developing Strategies to Counter It

Peter Bradley, Founder & CEO
info@torsionis.com     @torsionis
www.torsionis.com

Controlling insider risk, automatically

Shortlisted for infosecurity EUROPE
UK’s Most Innovative Cyber Security Company 2016
What is the Insider Risk?

Let's put a frame around what we're talking about.

The likelihood and severity of regular, trusted staff members with access to information, maliciously or accidentally allowing that information to fall into the wrong hands, causing damage to the organisation.

**Who:** Regular, trusted staff members in the business (not IT administrators)

**How:** Either maliciously or accidentally

**What:** Allowing information into to wrong hands – not just to outsiders
How the Insider Threat is Different

The insider threat is quite unlike other cyber security threats.

Compared to external hacking attacks:

• Roughly equal split between accidental and malicious causes – not 100% malicious
• So, every staff member is a potential assailant
• Tends to occur at granular level, document-at-a-time – not entire systems or networks at a time
• Effective solutions are much closer to the business than IT
• Higher likelihood of occurring – each company averages 9.3 incidents monthly

Strategy Advice #1
Don’t think of insider like other cyber threats – it’s not.
Understanding Your Risks

The two main components of understanding any risk.

**Risk** = **Likelihood** \( \times \) **Severity**

- The likelihood of an incident occurring (average anticipated incidents per year)
- The relative impact to the business of an incident, if and when it occurs

In terms of *business impact*:

1 \( \times \) Severity:100 incident = 100 \( \times \) Severity:1 incidents

- 9.3 incidents per month add up quickly, so don’t just focus on ‘the big one’!
- Strategies must decrease likelihood, severity or both

**Strategy Advice #2**

*Analyse & score your risks by likelihood and severity.*
The Nature of the Insider Threat

The insider threat occurs when information management fails.

Information management: connecting staff with the information they need

Insider incidents: staff accessing information they shouldn’t have

The Insider Threat: When information management fails!

• The insider threat is more closely aligned to the discipline of information management than it is to technology

• Information Architecture and Governance typically prioritise usability, convenience & control – not security!

• To address the insider threat, we must start with how business information is structured and managed

Strategy Advice #3
Prioritise security in your Information Architecture and Governance
A framework for **understanding your risks** and **identifying your constraints**.

To understand insider risks is to understand how business information is created, evolved, stored and shared – and **how things can go wrong**.

**Strategy Advice #4**

Evaluate your realities and constraints, across all four dimensions.
Insider Threat Technology Landscape

The **types of technology** which address specific vectors of the insider threat.

**Access Management** – controlling and reporting on who has access to what, and how that changes over time

**Data Classification** – classifying information by some combination of criteria, such as sensitivity, audience or purpose, and using those classifications to drive behaviours in people and technology

**Data Loss Prevention** – detecting, alerting and preventing documents containing sensitive details (e.g. CC numbers, DOBs, etc.) when moving across boundaries or between people in violation of business rules

**Behavioural Analytics** – monitoring user interactions with systems and information, alerting administrators to anomalous behaviour. e.g. trigger an alert if a user tries to download an entire document library

**Rights Management** – enforcing rights to interact with information in different ways, including when the information has left its host system. e.g. may only open a document if have rights, even off the network.

---

**Strategy Advice #5**

**One step at a time:**

1) **Score & rank your risks**
2) **Reconcile with your constraints**
3) **Choose most relevant types of technology**
4) **Identify suitable vendors & products**
A need-to-know access governance policy for all information is the most fundamental best practice.

Following the ‘Panama Papers’ breach, many experts have spoken on best practice for insider security:

“Companies should regularly review their access controls to see who has access to what information, and whether or not that access is still relevant to peoples' roles”.

- Brian Honan, Head of Information Security, BH Consulting

http://www.bankinfosecurity.com/panama-papers-6-security-takeaways-a-9018

Everyone with access to only what they need (and no more) = Minimising the ‘Insider Attack Surface’

Strategy Advice #6
Need-to-know access policies minimise the insider attack surface.
Over 70% of staff can access information they shouldn’t have
Thank you