The Swiss Cheese Security Pattern

Why it is important to take a pragmatic approach to security strategy, design, and implementation.

John Q. Martin

He | Him | His

Senior Data Engineering Consultant

Advancing Analytics

Speaker Info

John Q. Martin

(He | Him | His)

John is a data platform and cloud specialist with over fifteen years of experience. Working with Azure and AWS technology to deliver successful outcomes for clients in multiple industry verticals.

John@AdvaningAnalytics.co.uk

/in/johnqmartin

/johnmart82

Agenda

Security Strategy and Mindset.

First Principles of building secure systems.

The Swiss Cheese Pattern Vs. the Onion.

Strategy not Strategies

You should have one strategy which guides you.

Security First Vs. Secure by Design

Strategy

We will secure our business assets using approved technologies to meet our compliance obligations under GDPR, PCI-DSS, and Cyber Essentials. The approach will balance the risk appetite of the business with the usability requirements of the systems involved.

Strategy

What is the strategy window?

What and how will you measure the effectiveness of the strategy?

Set a review schedule to make sure your strategy is working.

Security is a state of mind

Do you understand how to approach and handle risk.

It's a case of when not if.

Plan for the worst, expect the best.

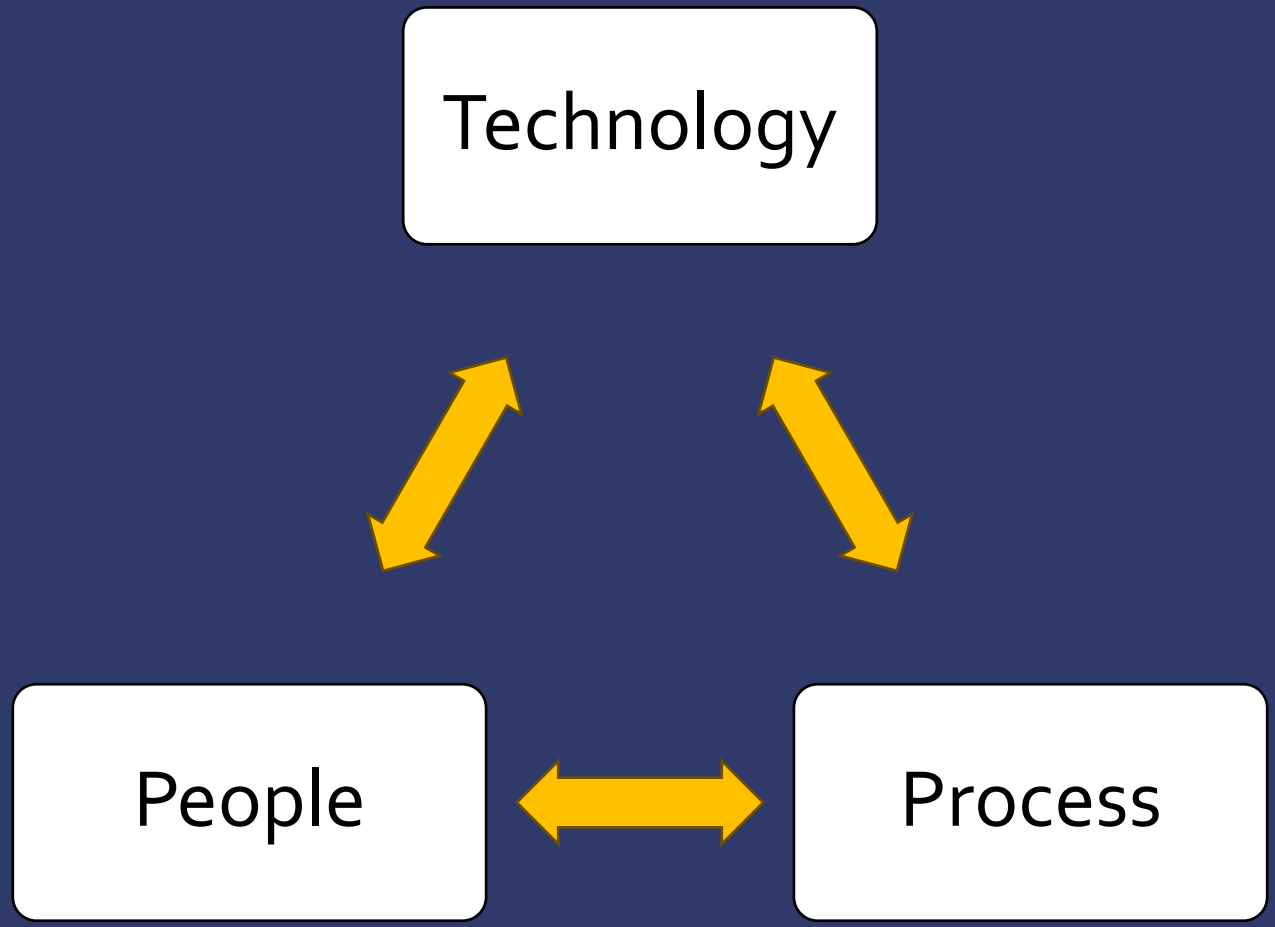
Taking a systems approach

Security needs to be baked in, not an afterthought.

Taking a systems approach is key.

Looking to achieve an overall balance.

Taking a systems approach



The Onion Analogy

Layers around the protected core.

Layers are complete, giving a false impression of security.

The Swiss Cheese Analogy

Layers are from top to bottom.

Each layer has holes in it, they need to be arranged so they don't line up.

The layers - Access

Physical Access & Location.

Network Access to resources, source to destination.

Lateral movement and Zero Trust patterns.

The layers – Authentication

Identity Provider such as Entra ID, Okta, AWS IAM

Application or Service based ID management.

API Key, PAT, SAS, etc.

The layers - Authorisation

User Vs. Role.

Granularity of authorisation and inheritance.

The layers - Software

Integration with authentication providers.

Integration with authorisation model.

Maintenance and vendor support.

My biggest security worry

The impact of encrypting or destructive malware which spreads within an environment.

Destructive attack recovery process.

Summary

Single strategy which guides the operational outcomes for design and implementation of IT systems.

Take a secure by design approach which balances user experience with risk assessment based approach to security.

Each security layer will have intentional holes created for functionality as well as potentially having unknown holes due to vulnerabilities.