e2e-assure

C.A.F. v3 - A Hitchhikers Guide

In your travels through cyberspace, the 5 things every hitchhiker should do first & why

This must be Thursday,' said Arthur to himself, sinking low over his beer. 'I never could get the hang of Thursdays.

Douglas Adams – Author – a Hitchhikers Guide to the Galaxy

Secure by Design

Nothings technically changed from the last one

And its only common sense anyway

Secure by Design

The following is my opinion only

In any journey its always wise to look for the shortest or easiest route to make ground quickly, this may change your direction of travel initially but the destination should remain the same

Secure by Design

A common mistake that people make when trying to design something completely fool proof is to underestimate the ingenuity of complete fools.

Douglas Adams – Author – Mostly Harmless

Secure by Design

#1

A1.a Board Direction

There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.

Why is this a Priority?

Because you need:

A powerful Sponsor of security projects - A Board level "friend" who gets what you are doing and can represent your position to the board

A referee to overcome inertia from other parts of the organisation

A funnel for budget

Secure by Design

A1.a Board Direction

This is #1 – because before you do anything…

You need someone to apply pressure to stakeholders when you need it applied, to get things done

You need some who can take ‘too much pressure’ away from you and your team to maintain programme focus

You need money and resource to do it regardless

Secure by Design

#2

A3.a Asset Management

All assets relevant to the secure operation of essential functions are identified and inventoried (at a suitable level of detail). The inventory is kept up-to-date.

Why is this a Priority?

Because you need:

To understand what your asset is, what it's doing and how critical it is to your organisation

To know if it is easy to exploit

To be able to scope what you, or more importantly, what a supplier needs to protect

A baseline asset inventory to identify any movement you can't account for (trackability)

Secure by Design

A3.a Asset Management

This is #2 – because before you go any further…

You need to know what you are protecting

Why you are protecting it

What happens if its compromised(Impact)

What vulnerabilities does the asset have(Risk)

How do I fix it (Programme)

What's the cost to fix (budget)

Who owns the asset (wallet)

Use your monitoring solution help to inform you of your asset base

Secure by Design

#3

A4.a Supply Chain

You can clearly express the security needs you place on suppliers in ways that are mutually understood and are laid in contracts. There is a clear and documented shared-responsibility model.

Why is this a Priority?

Because you need:

To know the roles and responsibilities for every element of your security posture including the bits looked after by 3rd parties

To be able to express that responsibility upon procurement

To be able to clearly articulate that in a commercial agreement

To be able to measure that the desired outcome of the procurement is being met by the supplier

Secure by Design

A4.a Supply Chain

This is #3 – because before you outsource…

You need to know that the organisation you are employing cares (is motivated to care) about your security as much as you do

Make sure your SOC can follow your data into a 3rd party environment

NEVER – OUTSOURCE A PROBLEM

Secure by Design

#4

A2.a Risk Management Process

Your risk assessments are informed by an understanding of the vulnerabilities in the networks and information systems supporting your essential function.

Why is this a Priority?

Because you need:

To be able to prioritise the action you will take to address these vulnerabilities

To be able to assess whether these vulnerabilities are inevitable to allow the system to function

To understand how the vulnerabilities you find can be exploited by an attacker and the TTP's they may utilise

To be able to create preformed responses to mitigate the risk of attacks utilising those very same TTP's

Secure by Design

A2.a Risk Management Process

This is #4 – because before you consider incident response…

You need to know what TTP's may be utilised to exploit vulnerabilities on your network

This approach will prioritise the playbooks you will need to author and implement and at the same time make them relevant to your essential function vulnerabilities

Secure by Design

#5

B4.a Secure by Design

The networks and information systems supporting your essential function are designed to have simple data flows between components to support effective security monitoring and be easy to recover

Why is this a Priority?

Because you need:

To start now – every change to an existing network or implementation of a new network should be designed to be secure, simple to monitor, easy to recover and resilient

To transform your legacy network to be secure by design over a period of time

To realise that attacks will happen and you will be judged on how quickly you detect, arrest the attack and how quickly you are back up and running again

Secure by Design

B4.a Secure by Design

This is #5 – because this one has a knock on effect on everything else you are likely to do…

It should be the mantra of every IT Manager everywhere

Introducing simplicity WILL reduce the cost of securing the network, thought in advance leads to a reduction in expensive changes to accommodate security

Secure by Design

Finally

The Cyber Assessment Framework makes sense but by it's own admission it is driven by the peculiarities of your own environment

While it provides a framework of outcomes that you can use as a measure it states that it's really down to your regulator to make that call

Secure by Design

Advice

1. Use the outcomes (IGP's) in the CAF to drive security procurement – a good supplier/partner will work to outcomes and should commit in the contract

2. Start somewhere (the CAF provides a good template) but realise that money may be tight or re-prioritised at times so do the things that have the biggest impact at lowest cost

3. Consider a cost effective monitoring and SOC solution early in the journey not only to monitor against bad things happening but also to inform the development of your capability and posture

Secure by Design

“I've come up with a set of rules that describe our reactions to technologies:

1. Anything that is in the world when you’re born is normal and ordinary and is just a natural part of the way the world works.
2. Anything that's invented between when you’re fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it.
3. Anything invented after you're thirty-five is against the natural order of things.”

Douglas Adams – Author – Salmon of Doubt

Secure by Design

Secure by Design

e2e-assure

Thank you

Secure by Design