thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 1

Introduction and Principle 1 - GOVERNANCE

This is my opinion

Please treat it that way, don't hate or criticise it, sometimes opinions don't align but hopefully you will find a large helping of sense in these outbursts, if for any reason, however, you do disagree, please reach out, having your own opinion is what this document is there to drive.

To the reader,

Welcome to my opinion – it's a scary place sometimes but hopefully the series of outbursts will add value or at least get you to think of Cyber in a different way.
Yes, you read that first bit correctly, this is a series you are about to embark on, stick with it if you can.
Yes, we are going to highlight Cyber (zzzzz – wake up!) this has probably been done to death, but you never know.

So here we go...

Before you, intrepid reader is the first of 14 documents (14!), I am going to try and explain why the approach you take to increase your cyber resilience and therefore, your business resilience to cyber risk and your customers trust in your brand can be improved by following a framework and more importantly, why you would invest your time and resource in it.

First thing to note – the framework you use is incidental! Sure, it needs to align to your industry (if regulated), it needs to be proportionate to your risk profile and business model maturity, of course, but you couldn't squeeze a cigarette paper between most frameworks, however, some are more technically oriented and deeper in detail than others and some won't apply to your industry or market geography.

For this series I am going to pick on NCSC's Cyber Assessment Framework (V3.2), why? Because it's easier to navigate in an opinion piece, largely however the principles I highlight can be applied in pretty much all of the headline frameworks.

Remember this is an opinion, I am happy to be challenged and if you do, I at least have the comfort of knowing someone read it.

Why 14 bloody documents Stu?
Good question, seasoned travellers of my untamed rhetoric will answer for me, but I wanted to take each of the 14 principles in NCSC's framework in turn, to give you what I think is a good bite size exploration of it all (and not just focus on bits).

Ok, strap in.

Framework structure

Objectives, Principles & Outcomes

The framework is broken down into 4 areas (objectives), these are:

1. Objective A – Managing security risk
2. Objective B – Protecting against cyber attack
3. Objective C – Detecting cyber security events
4. Objective D – Minimising the impact of cyber security incidents

Each of these areas carry principles, there are 14 of these spread across the framework and under these sit 39 outcomes (I've seen that 39 reference somewhere before...)

Indicators of Good Practice (IGP's)

Everyone loves a good acronym! IGP's, these are statements of practice that indicate whether an objective is being achieved, partially achieved or not achieved, there is a danger that if these are assessed internally then they can be worked around to

demonstrate good practice, equally they should be applied with knowledge of the business model of the individual organisation – that's my opinion of course

Today I will be focussed on the first principle – A1 – GOVERNANCE – why it's important and how good practice here enhances the efficacy of other principles.

Governance

The first thing to say is that governance should be effective for your business – don't think because Joe Bloggs PLC is using 'this structure' means it is right for you.
Whilst for some this is a dry subject (I don't disagree) it's a necessary function that underpins any business posture – you'll notice I didn't say the word 'cyber', that's because governance is bigger than that, however, the framework in this case is only really interested in avoiding business disruption from cyber-attack and because this isn't a novel I'll cover that bit.
It is worth saying, however that cyber governance should take its spot in the overarching business governance of any organisation and should be considered alongside it and in the boardroom, the CEO should be as aware of it as much as the CISO or IT Director, having that spot at a board meeting is vital for any cyber maturity programme to thrive.

The 3 outcomes you want to achieve are:

1. Direction: Having effective security management at the very top of the organisation – this is not somebody else's problem, it theirs.
2. Roles & responsibilities: Ensuring that the board have skin in the game when it comes to cyber security and understand the part they play in managing that risk, yes they have a role here.
3. Decision making: Making sure that senior level accountability for operational security is part of their day job and that they are effective, after all the trading continuity of their organisation is dependent on it.

So why are these things important

These outcomes force the board to take notice and place cyber alongside other risks in the business, this is a good thing, right?

Why are these outcomes important

Let's tackle number 1 first – all too often cyber risk is pushed to the IT community (if there is a community) and then forgotten about by the board.

IT and security professionals struggle to achieve progress in improving the cyber posture because, when its invisible to the board, securing budget, resource and support in a maturity programme is difficult at best.
There needs to be a moment where the connection between brand trust and cyber security effectiveness needs to dawn on the board.
Now I am not saying that all executive members are the same, far from it, but the approach is at least inconsistent, asking your IT team to fix a problem that you are not prepared to commit to at board level starves the programme of resource and increases the stress levels of the poor soul in IT that can see the problem, knows how to fix it but is given no ability to do anything about it.

Imagine you are being asked to disarm a bomb, you know what colour wire to cut but no one has given you the wire cutters... tick tick tick...

A more nuanced implication of board awareness or rather a lack of it in the inertia this creates around policy review and security policy creation, most execs steer clear of "tampering" with the fundamental spine of the operation. To meddle is too risky, without an understanding of the implication of cyber security and its underlying impact to policy, the board will baulk at fixing something they believe doesn't need fixing, ergo, they won't invest.

Ok, on to number 2 – lets stand back and start with the phrase "roles and responsibilities", how many of us have well defined and definitive roles and responsibilities relating to the tasks we carry out in the job we do, there's probably a good LinkedIn survey there (and its probably been done many times), I won't stun you with empirical statistics on the subject but I guess we all know that we do things that aren't in our job description and don't do things that are (broad accusation, I know that but place your hand on your heart and tell me honestly that that isn't true).

When those roles and responsibilities are operationally critical for an organisation, however they should be known and reinforced, I would say.
If these are not conveyed (and they apply from top to bottom in an organisation) then you'll lose focus.

The problem tends to be, more so in smaller organisations, that roles are filled by people that may not have the appropriate skill to be responsible – this is not unfixable, but it takes time and/or money.
Importantly though for you the reader is that if cyber maturity is to be taken seriously then the roles and responsibilities to create and maintain that posture need to be in place and if they're not, then implementing the strategy to create operational resilience will falter.
Remember the board and the user at each end of the spectrum are part of this and critical to it.

Well, that bit sounded a bit preachy, but I am trying to make a point, I guess.

Finally, for this document at least, Number 3 – Decision making...

I speak to a lot of people about this, or rather, it comes up a lot when I do.
"The board never make decisions quickly and this stops me doing what we need to do to secure the business and respond quickly to a changing threat." Heard that before? Said it yourself?
Stop blaming the board.

If that sounds a little unfair, consider this. Which member of your board is the well qualified cyber security expert?
Unless you are a small cyber company, then probably the answer is none of them.

I am going to keep this simple – people don't make decisions when they don't know what they are making a decision about and organisations don't invest in stuff because someone told them they should but didn't explain in terms they understand, why?
The why isn't technical or process impacting or because someone else did this, the why is how it makes the business more viable (that means profitable and sustainable).

Oh, and delegating decision making is a top end decision, which means you must convince the person delegating in the first instance.

Maybe you are the problem...

The trick is to learn the boards language and convey your asks accordingly and risk decisions need to include real world impacts to the business' brand trust and resilience.

Help on this is never far away, find an internal sponsor to work with who speaks the boards language (and is on the board), CFO's and COO's are a good target.

Never be shy of looking for advice here, it's important and this bit impacts everything else we will talk about in this series

Ok so I hope that all made sense, I'd love to hear from you if you agree or disagree, this is however, only my opinion, if though you do agree and want to discuss a particular area in more depth you can reach out to me at stuart.avery@thirtyninecyber.com

Like this? Please follow ThirtyNines LinkedIn page – https://www.Linkedin.com/company/thirtyninecyber and read more in this series as they are released