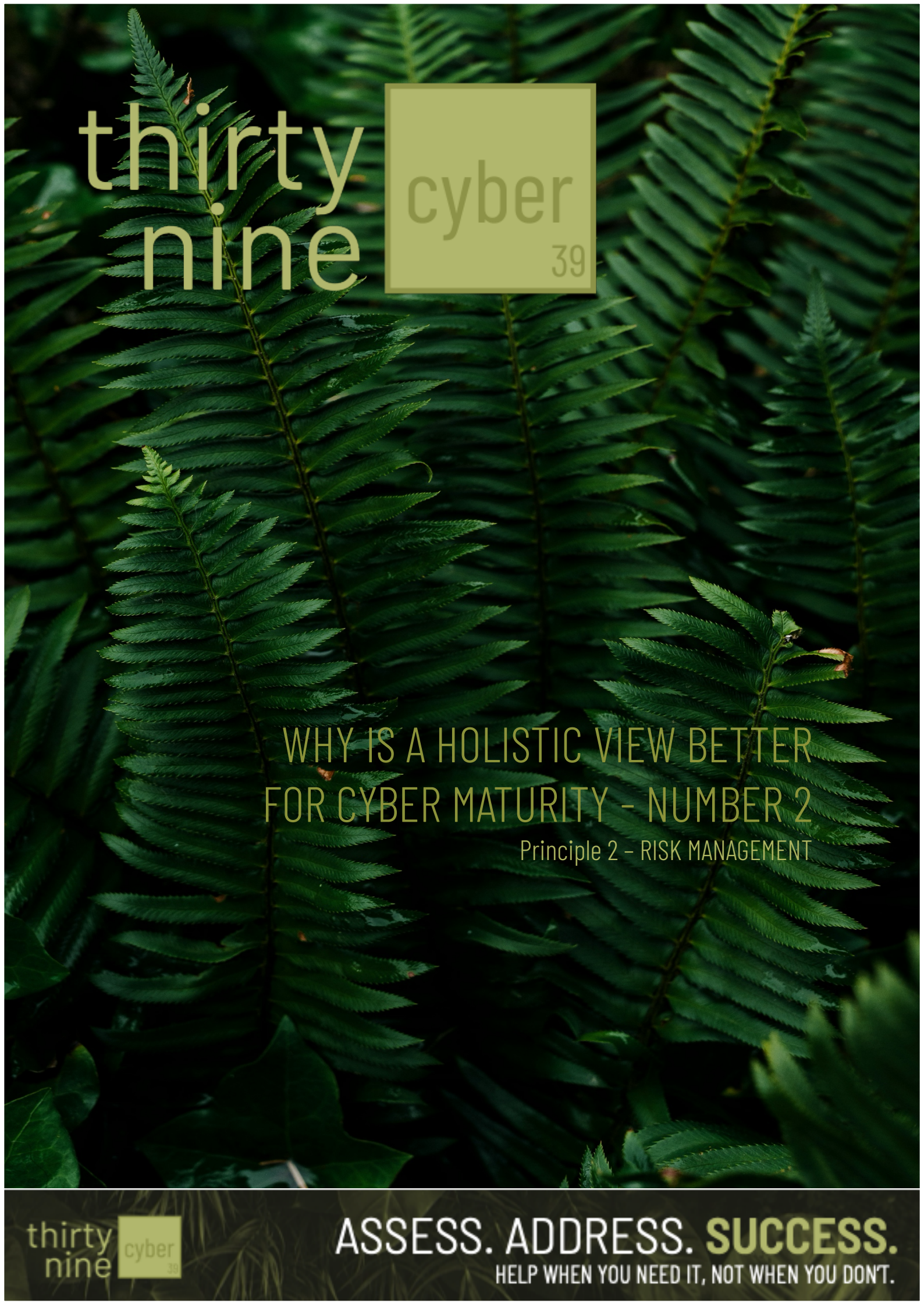

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 2

Principle 2 – RISK MANAGEMENT

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...

This is the second one in the series – I want to start with an observation on my own lack of a grasp on the English language, I used the phrase Wholistic in the title of the first post... Ok, so Word didn't help me and neither did QA, I have been pulled up on it, Holistic is the correct spelling, or is it, I have also been told that either spelling is fine... go figure - I have changed it anyway.

I am going to focus on the second principle in NCSC's CAF framework.

Remember this is meant to give a high-level view of why this bit is important to an organisations maturity and how this element impacts other areas and controls on the route to achieving cyber one-ness.

It isn't designed to be technical, it's meant to help you, the reader, to understand why we bleat on about assessing holistically not in parts.

If anyone comments about the spelling of "Holistic" I might just use "complete" ...

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 (IGPs)

Everyone loves a good acronym! IGPs, 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 second principle – A2 – RISK MANAGEMENT – why it's important and how good practice here enhances the efficacy of other principles.

Risk Management

This section is super important, not just because it's got risk in the title – no one really likes risk, it's about how risk is treated.

Let's start with a controversial statement:
Cyber risk is NOT IT risk, it's NOT an IT problem. If you disagree with that statement, then you definitely need to read this.

Here's my view.
Cyber risk is a business continuity issue and a brand issue, not rocket science really when you think it through. If you are compromised and either your critical system is unreachable, you lose customer or IP data, your bank balance is drained or you become a host to a nefarious actor that uses your digital resources as a launch pad for their "mission", it's the continuity of your business and trust in your brand that suffers.

Once discovered or made public (and the bad guys will let everyone know), do you think your profits rocket?

Good luck if you believe that.

There are ways of thinking about cyber risk and how that risk is, firstly, recognised at all levels within a business and secondly, treated in line with broader business risk. My commentary below might add a little insight into what we and others believe is best practice and why you should try to achieve the two outcomes aligned to this principle.

The 2 outcomes you want to achieve are:

1. Management Process: Making the business risk process inclusive of cyber risk that is up to date (in line with the prevailing threat landscape) and coupled with a clear process to mitigate that risk (have a strategy)
2. Assurance: Ensuring validation of the mitigations in place with measures that are simple, effective and prioritised (have a programme).

So why are these things important

Placing cyber risk alongside other risks in the business, adds context, it creates a board culture that treats risk and makes resources available as it would or should do for other external forces that might impact business profitability.
Cyber investment is NOT a cost centre or an insurance policy, it's a profit enabler and once embedded becomes second nature.

Always the inertia lies in best practice adoption, but the payback is worth the effort.

Why are these outcomes important

Let's get started - Number 1 – all too often cyber risk is pushed to the IT team (if there is a team) and then forgotten about by the board. That's how I started with the last document (if you haven't read it, go to our website – it's in the opinion section), it demonstrates that the journey to cyber maturity is inter-dependent it's a winding road that needs focus and sponsorship to navigate.

We also talked about decision making, a risk management process that is simple, clear in its call to action and adopted by the board, enables members who are not cyber experts to make decisions quickly, it also drives the cyber stakeholders to ensure they make mitigation proportionate and realistic to deliver.

Risk impact should detail how business sustainability, brand trust and profit is affected, this will help the board to understand the fundamental issue.

It's important to note at this point the key principle of risk management and the process to convey and quantify it – it needs to be up to date.

You can't sit on a risk register and think that it retains currency when the world and the threat that lives within it, changes. Technology advances, geopolitical forces, changes in activist focus or even a product or profit announcement can attract unwanted attention – not great right?

Risk is a moving beast and needs shepherding appropriately, any process you adopt to manage it needs to consider that movement.

Where I have seen risk management work best is where the company don't hide from it but rather give it ownership at board level, place it alongside broader risk and create responsibilities for senior members to drive mitigation and review the register and threat landscape regularly, once adopted this area is the lynch pin around which maturity is mobilised. Remember you need to understand where specialist input will be sourced to ensure risks are relevant to your organisation, don't be shy, ask.

Which leads me nicely on to the next outcome. (It's like I planned it...)

Ok, on to number 2 – Assurance, for this bit I am going to focus on the validation of firstly, the risk and then the action you will take to mitigate that risk.

Is the risk relevant – an example:

In the manufacturing industry the biggest risks of disruption were around production line disruption and supply chain continuity. It tended to be that production lines were air gapped (not connected to external networks) and pretty fault tolerant. If they were compromised by an internal actor, it didn't carry much of an impact, the supply chain wasn't critical, most raw material was ordered from various sources over the phone and the materials were stock piled, usually in an adjacent warehouse.

Risk of disruption from digital compromise was low to non-existent, but the world has, and is still changing, connection of production systems to cater for customer demand spikes and just in time supply mechanisms to reduce cash tied into stock (in the drive to increase profit growth and reduce cash flow issues) means that business resilience is dependent on ensuring system continuity.

By the way, the industry has to connect to be competitive and there are lots of pressure points right there.

So not that long ago, cyber disruption and measures taken to avoid it were not necessarily at the top of the list, today denial of access to connected ordering systems and production line processes can be catastrophic and if you're part of a critical supply chain, the impact to brand trust can sink profits almost overnight

So then risk needs to be relevant to your business model as well as to the threat landscape.

This adds a necessary step, Assurance.

You need to make sure that the risks you perceive are real, relevant and the mitigations you prosecute are valid, effective and actionable.
Having an external advisor, whether that's an authority or a security partner is critical. Remember the outcome here drives the maturity programme you embark on; you want to keep the cost in check and ensure the benefits are clear.

Also join forums to see how others tackle the issue or advisory organisations who can reduce your security total cost of ownership with sage advice, prioritisation and proportionate approaches – remember don't panic, look first, leap later
Never be shy of looking for advice.

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.