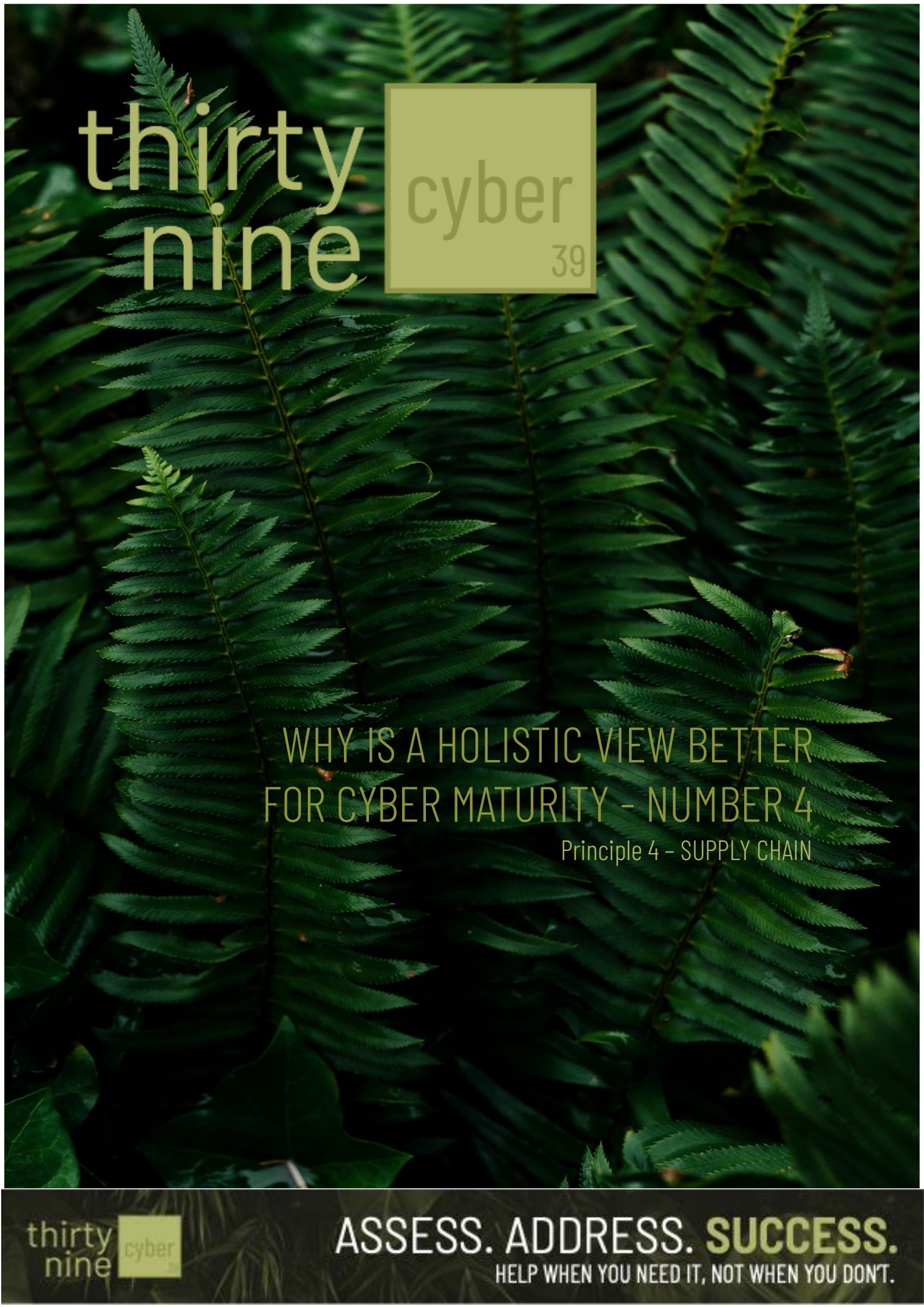
thirty nine
cyber 39
WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 4
Principle 4 - SUPPLY CHAIN
thirty nine cyber
ASSESS. ADDRESS. SUCCESS.
HELP WHEN YOU NEED IT, NOT WHEN YOU DON'T.

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.
This is the fourth one in the series – covering the fourth principle in NCSC's CAF framework – Supply Chain.
Remember this is meant to give a high-level view of why this bit is important to an organisation's overall maturity.

So here we go...

Key takeaways

I have discovered that sometimes people don't want to invest in reading the whole document unless they have a good idea of what it covers – ok fair, so I have added a new bit to give you a summary view.

So, what's in it

1. Why is supply chain risk management critical
2. How can you do it without destroying your margin and compromising the operational continuity of your organisation
3. What you should consider when employing a supplier
4. How should you apply obligations without scaring the horses

Still fancy reading it?

Ok, strap in.

Supply Chain

NCSC's CAF deals with supply chain in one small section, one principle, this hides a simple truth, doing this bit is hard and carries some of the most significant risk in any organisation.

A good place to start is to understand why it's called a chain, like any chain each link is dependent on the other, a broken link stops the chain from being functional and that means you are not just thinking about the link that represents you, that's why it's hard, because now you have to think about the other links in the chain. I know that sounds obvious, but I don't apologise for stating the point.

It's not easy to tackle then, but that doesn't mean you shouldn't and just reading your suppliers boilerplate security statement is not enough, you owe it to your customers/citizens to validate the supplier's maturity and to understand how much risk the supplier represents to the continuity of your operation.

So why is the Supply Chain principle important?

Outsourcing elements of an operation is common, in our drive to reduce cost and therefore increase profit and to reduce the headache of building specialist teams in-house, it's a generally adopted practice.

There are some gotchas though, these might sound obvious, but they are worth saying.

1. You have a responsibility to your customers and employees to look after their data, you cannot outsource that responsibility.
2. You may be giving access to your networked environment to an external organisation that could, if not properly secured, act as an open door into your core operation.
3. You will extend the scope of your security function into another organisation where they will have little visibility

4. You may want to extend operational and brand risk responsibility to another company, they won't accept it, and you will find any operational or brand disruption liability difficult to enforce without the proper commercial agreement in place.

If this last point relies on additional obligations being applied in a contract, even in retrospect, the cost of the service is likely to go up, impacting one of the reasons for doing it in the first place.

I am not saying outsourcing is bad

What I am saying is that management is key, so in turn this principle is key and one of the more important principles in the framework in my opinion.

Things to consider

If you have outsourced a critical or Important Function of your operation, you need to make damn sure that the function is at least as resilient as it would be if operated in-house, that might not be a high bar for some, but you can't outsource risk and you can't expect a supplier to run your function without some assurance that they are meeting a standard.

You can think of supply chain and the management of it like asset management on steroids.
Like asset management the first place to start is to understand your suppliers and where they fit in the operation of your organisation. How critical are they to the continuity of your operation?

Why? Because you can understand what assurances you seek and what obligations you flow down to them, relevant to the function they operate on your behalf – this element is important if you want to manage cost or avoid making the contract between you, unsustainable.

Supplier categorisation – PUT YOUR EGGS IN THE RIGHT BASKET. Clearly, knowing the asset that supports your critical function is a necessary thing. That doesn't change just because it's somewhere else and lives in another organisation. Who, therefore, holds the asset (physical, people, data)? If it's a supplier, then a greater level of assurance needs to be applied. Don't focus on suppliers that aren't in this bracket immediately, there may be a simpler way to assure them, that saves business effort and management cost.

Considerations – The things that are important to consider when categorising a supplier.

1. Interruption to your service or productivity if you cannot access the thing that the supplier provides due to a cyber incident – does your supplier operate a system accessed by your core service or directly to a client – if they stopped would you stop?
2. Do they hold data (critical PII, IP, confidential data or above) on your behalf? – You can't outsource the risk to the security of this data.
3. Would a supplier-side cyber compromise impact YOUR brand? – Don't leave this one to chance.
4. If the supplier went down and stayed down, could you recover that element of the service quickly by either moving it in-house or accessing another supplier and would the architecture you employ in the provision of the service allow you to move the operational role quickly?
5. Do you have a BCDR plan that details all of this?

There are other considerations (and certainly technical considerations that I haven't begun to tackle here) depending on your business model, I am not going to second guess what's relevant to you here but if you know your operation and what's important to it, then you will naturally add other considerations.

Asking those questions internally first, gauges your supply chain risk impact. Not the probability I hasten to add, your onward conversation with your supplier and how they maintain service continuity and the architecture they wrap around it will define risk probability – that's the next step.

Finding the balance in supply chain.

To achieve this starts with an honest conversation with the supplier, either through an impartial assessment (fine) or peer to peer conversation between CISOs, security professionals or IT teams.

It won't benefit you to over play obligation flow down as a blanket exercise, imposing the toughest stricture to all suppliers, they will either up their price to provide (which may be necessary) or they'll walk away because they can't make money (oh and by the way, that's why they do whatever it is they do).
Start with the most impactful suppliers first, have a friendly conversation about your concerns, understand their business model to define the red line for them, the contractual relationship needs to work for them too.
Critically understand and map the data flow between both organisations, find out what controls are in place to protect it.
Agree with input from the supplier, the assurance framework you will be applying and tell them why (help them understand your business model). And if necessary, detail and document a joint service specific BCDR plan to shorten any risk.

Only apply what is necessary to the individual supplier based on their risk profile and how you have categorised them.

Balance is critical to maintain cost and keep your CISO from burning out, whilst maintaining continuity and retaining brand trust.

Like I said I could write all day on this subject, there is so much I haven't covered.
My advice: Take some time on this bit, seek guidance if you are unsure how best to approach it and don't think a tool or draconian obligations are going to fix it

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.

Appendix One - Framework structure

Objectives, Principles & Outcomes

Largely a good assessment is a good assessment, the framework is largely incidental but as we're talking about CAF, I have written this summary

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.