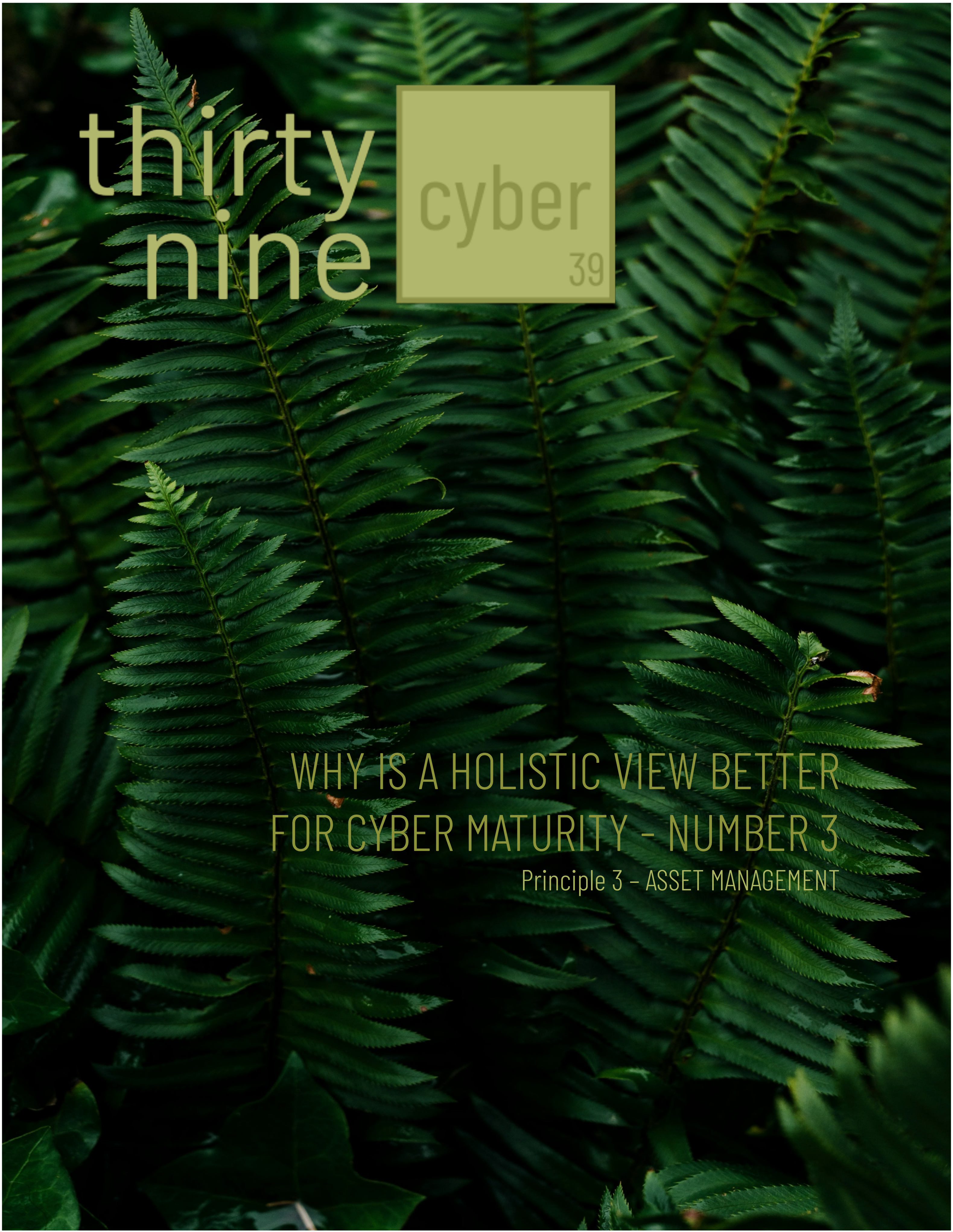

thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 3

Principle 3 – ASSET 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 third one in the series – In this one I am going to focus on the third principle in NCSC's CAF framework – Asset Management.

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.

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. The document positions asset management, what it includes and how it plays a vital role in maintaining security.
2. Helps to understand why the state, location, and criticality of assets is essential for effective risk management.
3. Highlights the data obligation and why understanding what it is and where it is, is critical
4. Touch on how to mitigate risks related to asset control.

Still fancy reading it?

Ok, strap in.

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 very brief 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.

Asset Management

NCSC's CAF feels a little lightweight here, at least outwardly. To the skim reader you can be past this principle in the blink of an eye and the IGPs feel loaded towards the physical asset.

Asset management comprises of a few elements, some are focussed on by organisations more than others, before everyone cries foul, this is my observation only.
You should consider your asset as:

1. Physical or system asset – this is the one people tend to think of first, this basically covers system hardware, firmware, OS and software, these assets usually form part of a register that includes versioning, criticality and dependencies, good ones will also define vulnerability and system network impact.
2. People – sometimes overlooked, understanding your critical and key people, includes detail of system ownership and responsibilities is hugely important, you will need this map to succession plan and to understand your capability risks.
3. Data or information – this is the puppy that is either left to chance or not understood in a lot of organisations, but this one is vital to the security of your organisation, I am going to talk a lot about this below

So why are these things important

I am pretty sure that knowing what you have, what state it's in and where it is, is important and I think we all know that. If I asked you what your wallet or purse looked like, whether there was money or cards in it and where it was, you'd probably know or at least would have a good idea (or if you didn't, you're probably panicking now… sorry).

Your organisations asset is no different.

The CAF details your desired outcome as: that the asset required to keep your business alive is determined and understood. I'd add that anything that supports the personal safety and identity integrity of individuals is even more important, but that's just me maybe.

Why are these outcomes important

Physical or system asset management – clearly, knowing the asset that supports your critical function is a necessary thing. Its current condition, where it is, how it is accessed and its criticality should be recorded and then managed effectively (patched, monitored, etc.).
Most organisations will do this in the core of their system environment but maybe less so on the edge (mobile being a slippery area in particular). Knowing the status of your physical asset allows you to be more pragmatic in your approach to risk management, enabling you to better understand the probability in risk, not just the impact.

People – not always considered and sometimes left to line management and HR, I feel this element has a place in the management of cyber risk, especially where management processes are not properly written down (and let's face it there is a lot of "ask john, he knows how that works" in every organisation).

Mitigation of this risk includes mapping people to process and ensuring succession plans are in place to combat attrition, as well as the obvious, write down the process bit.

If the answer to the question, does staff attrition weaken system management? Is a yes, you need to address it by doing this stuff.

Data or information – ok so this is the one that can cause problems, it's intangible to some but is important to the survival of your business. You will inevitably hold data, either as a creator & controller or a processor (these have implications in the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA)) these roles carry obligations on how you will treat the data, obligations that are impossible to meet if you don't know where that data lives.
Equally you have a duty of care to your customers and employees to maintain the security of their Personal Identifiable Information and maintain the integrity of their identity.
Understanding where the data lives is complicated by employing third party organisations to conduct operations, the data crosses to a place outside of your direct control, doing this carries inherent risk that should be mitigated by ensuring that the obligations you carry are transferred as part of the engagement, usually this is left to a trust mechanism detailed in a contract but can be validated by imposing certain controls, many use compliance mechanisms, ISO27001 or Cyber Essentials but transferring defined process requirements can also be used.
Remember that imposing processes and compliance on a partner can make the engagement more expensive and sometimes tricky for the partner to adopt, governmental defence departments will tell you this and their supply chain will tell you how tricky additional safeguards are to deploy, sometimes in organisation who can ill afford to adopt them making the contract unsustainable or forcing them to walk away.

There must be a happy place somewhere.

My view is to firstly define the data you are moving or storing. Map your data, how critical or sensitive is that data, what obligations have you committed to and what function does it perform. When you know this, understand where it lives and understand what data crosses your boundary into another place (oh and that includes cloud hosting services).

If you understand this you can make any obligations you flow down, internally through SLA's, controls and segregation or externally to a third party relevant and proportionate to the data you are passing across.
If your third party isn't holding critical data, don't impose disproportionate and restrictive obligations, it'll be more cost effective for you and allow you to maintain the right focus on the right data for the right reasons, reducing organisational overhead.

Good security decisions begin from understanding your asset and managing it effectively.

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.