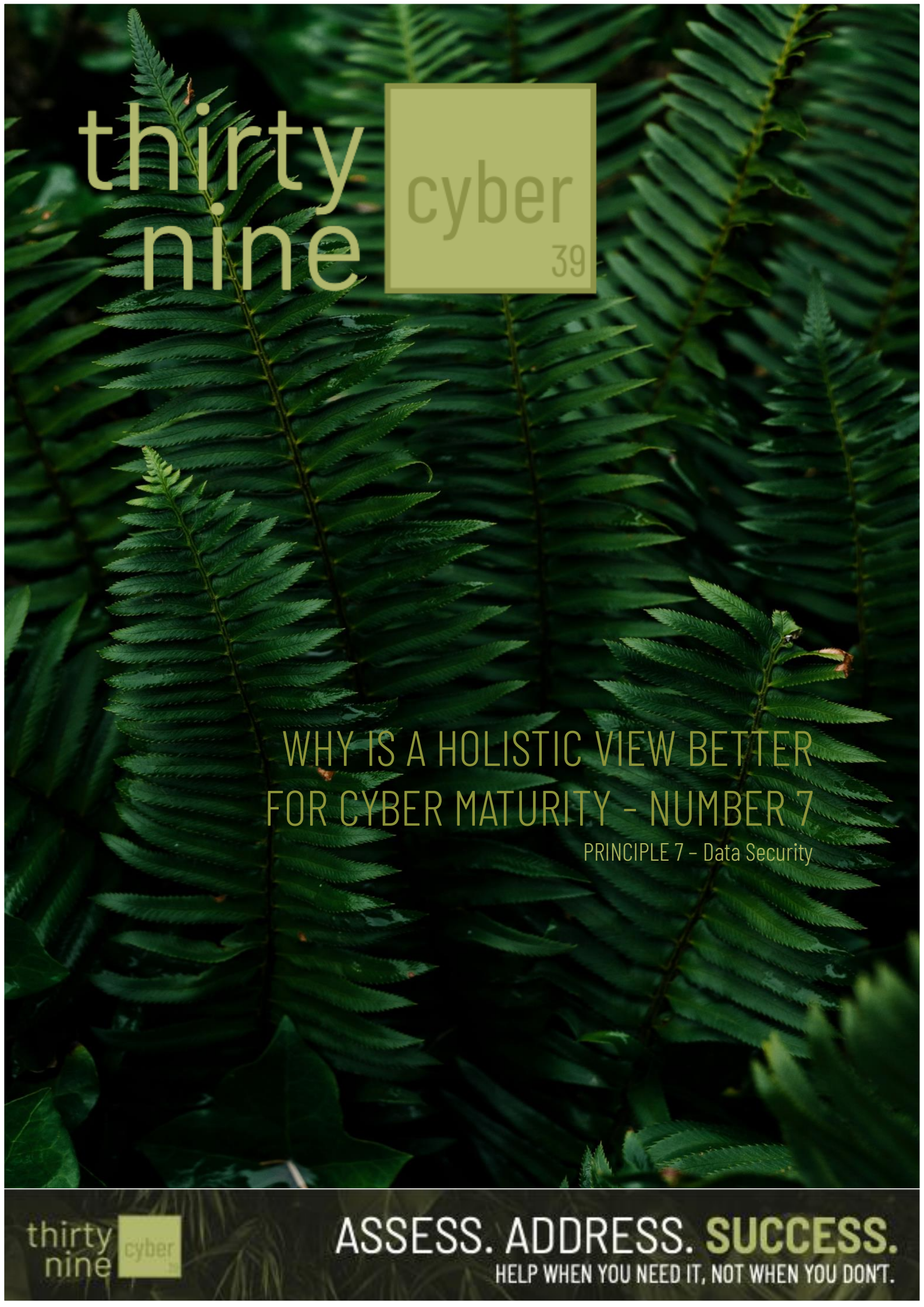
thirty nine
cyber 39
WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 7
PRINCIPLE 7 – Data Security
thirty nine cyber
ASSESS. ADDRESS. SUCCESS.
HELP WHEN YOU NEED IT, NOT WHEN YOU DON'T.

To the reader,

Welcome to my opinion – This is the seventh one in the series – covering the seventh principle in NCSC's CAF framework – Data Security.
Note: this is meant to give a high-level view of why this bit is important to an organisation's overall maturity. It's not exhaustive!

So here we go...

Key takeaways [TL; DR]
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. A scenario – to help crystallise the subject and its importance
2. Considerations to help you find the best approach to define your approach to data security

Still fancy reading it?

Ok, strap in.

Data Security

Wow where do I start!!!

Data is important; therefore, this Principle covers a lot of ground and is broken down into fundamental areas in the assessment framework

NCSC CAF states that to secure data, there are five outcomes that must be achieved.

a) Understanding data – have you mapped it to know how critical it is, where it is, where and how it's stored, how it gets there and can understand the impact of a compromise to its integrity?
b) Data in transit – do you secure your data when it's on the move?
c) Stored data – do you secure your data when it's at rest?
d) Mobile data – do you secure data held on mobile devices?
e) Media/equipment sanitisation – do you reuse and dispose of assets containing data appropriately?

I will try to call out these areas in the scenario used for the next bit, hopefully it will demystify the subject a little.

Why is the Data Security principle important

MAKING THE IMPORTANCE OF DATA SECURITY REAL
So, let's turn Data into something equally emotive but maybe more tangible.
Consider your data as money, cash, physical £££'s.
Now apply the CAF outcomes to your money and how you apply security measures to retain that cash.

You have money, it lives in different places and in different mediums.
This example demonstrates how you unconsciously treat the risk of loss, using three of the most common methods of cash transaction.
Paper, Plastic (Cards) and Virtual Cards (apple pay, google pay, etc).

Paper (although notes are more plastic these days but that would make this scenario totally confusing, you'll see why in a minute), not so common these days but you'll probably have some in a wallet or purse and maybe a coin jar (or maybe that's just me). – it's relatively easy to access, sure there's physical security provided by a pocket or bag (or jar... yeah, just me then), but a

wallet is easily lost, and paper money is impossible to trace (for a normal individual who hasn't marked their notes or put an RFID tracker on them, imagine...)

It's transferability and lack of security makes it more unattractive as a medium, your awareness of the location of the money increases when its value increases (criticality) – we grip tighter to a wallet with more money inside it.
UNDERSTANDING: GOOD
SECURITY ON THE MOVE: POOR
SECURITY IN STORAGE: POOR
SECURITY ON MOBILE DEVICES: N/A
MEDIA SANITATION: GOOD

Plastic (see? I said it would be confusing if I called notes plastic), more common but tends to live in the same places as paper, some plastic contains your money (Debit Cards), some, somebody else's (Credit Cards). Preferable due to an extra layer of security although compromised by contactless. The need to have additional credentials means that plastic is less attractive to someone looking to obtain your cash, the security of your money is further diminished by the advent of internet shopping.

Interestingly there is a generally adopted threshold for risk appetite built into modern cards allowing relatively simple access to around £100 via contactless, imposing the need for further credentials for anything higher.
UNDERSTANDING: GOOD (if you have visibility of your funds)
SECURITY ON THE MOVE: POOR
SECURITY IN STORAGE: POOR
SECURITY ON MOBILE DEVICES: N/A
MEDIA SANITATION: GOOD (but needs a phone call to cancel its validity)

Virtual Cards, becoming more common as seen by many as more secure and convenient (although there's a strong argument whether you just invite a whole new bunch of sticky fingered herberts to the party), these are accessed generally using biometric tech like fingerprint or facial recognition, but there is a failsafe (which can be selected) that uses the phone's general access code, so hackable, but, it's a layer of security in which the manufacturer has tried to find a balance between security and convenience.

With this method, there is no upper or lower limit to the cash you can access but you must overcome the security applied for any cash amount which means it's a step up from the others here, biggest risk – phone loss/remote hack.
UNDERSTANDING: GOOD
SECURITY ON THE MOVE: REASONABLE
SECURITY IN STORAGE: REASONABLE
SECURITY ON MOBILE DEVICES: REASONABLE
MEDIA SANITATION: GOOD

So why did I write this out, it's pretty obvious, we do it every day.
Replace money with data, replace medium (paper, plastic, vCard) with system.
When you want to use money (data) to buy something (function) by using a payment medium (system) you consider why? How? and the risk of doing so, as if it were muscle memory.

That's the ethic you need to adopt when handling data, who can access? Where does it live? How does it get there? Is it secure when it moves or stays still? When it no longer serves a purpose how do I dispose of it securely?

Remember it's not only about being hacked – if your phone ran out of battery when you were out shopping and you only use vCards, you're a bit screwed. Denial of access to systems is the same thing (that's ransomware's objective), so it's not only about loss, tampering or unauthorised visibility, it's about access too (Confidentiality, Integrity, Accessibility – CIA)

Things to consider

There are some simple considerations to make when handling data, whether that's yours or a third party's.
I have gone through some simple ones here (or least they are simple to say but maybe harder to do in some cases).

Considerations:

1. What data? - Before you apply the highest security to any data that moves or sits still, maybe try to understand it

Categorise the data and its importance – if you carry data that belongs to someone else defining criticality is not going to be your decision alone, so ask (organisations used to provide a Security Aspects Letter SAL to define how data must be handled – God I'm old).

Regulation steps in here too (e.g. GDPR) and removes some of the ambiguity around categorisation.
I would say that defining or re-defining a data policy is critical at this stage to match the data that you control or process and allows you to create proportionate responses to the CIA risk.

It's not straight forward sometimes and the task will depend on the number of systems and amount of data you host, do it if only to avoid the eyewatering security bills.

2. Where? - Understand where it lives or how it moves and why

   Equally important is to understand how many times that data has been replicated, data sprawl is a problem and it's not just the original copy that carries the obligation on you to protect.

   Like I said, easy to say, hard to do. Break down the task at a systemic level, start with critical functions and apply your data policy religiously, any overreach when applying the policy can be dealt with by exception.

   Map the data to understand how you add security controls to it.

3. Impact of compromise - define the risk it's simpler now you know what you have and where it lives or moves, risk will become obvious when you understand and map the data.

   Treating the risk will be defined by the impact and probability of the risk materialising.

   Make the risk clear and define the business benefit of mitigation simply and clearly, this is going to the board they are not necessarily cyber experts, but they understand business risk – it's their job.

4. DON'T DO IT ALL AT ONCE - chunk it up, not only will this save a visit to the asylum, but it will also give you a systemic perspective and allow mitigation in the same way.

5. Get help - this is not a rockstar task, getting another pair of eyes and a different opinion is valuable – involve third parties who own the data, understand their perspective and minimum requirements, it will help.

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 objectives 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.