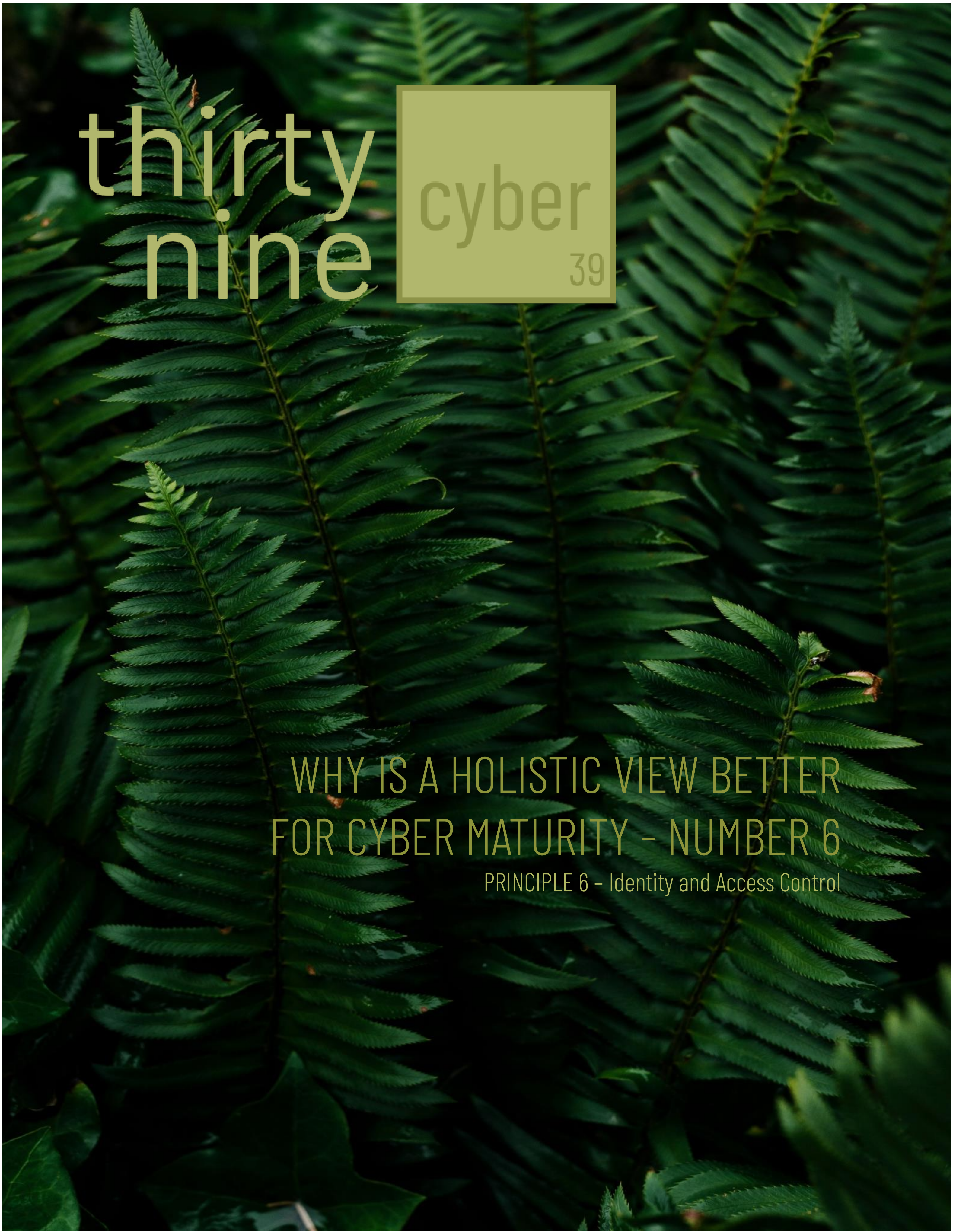
thirty nine cyber 39



WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 6

PRINCIPLE 6 – Identity and Access Control

To the reader,

Welcome to my opinion – This is the sixth one in the series – covering the sixth principle in NCSC's CAF framework – Identity and Access Control.
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. Identity Access, what is it?
2. Why implement it, why is it important?
3. Considerations, things to consider to make it effective.

Still fancy reading it?

Ok, strap in.

Identity and Access Control

This area has received a lot of attention over the past couple of years, helped along by the move to micro-segmentation and zero trust in network environments.
Validation has moved from the device to the identity of the user/administrator and has used out of band authentication methods to reduce the risk of device compromise (tokens, Multi Factor Authentication, One Time Passcode, etc)
The underlying goal in simple terms is to make sure that only the right people can access an organisation's systems and data. Access can then be focussed to a user's role or need and changed dynamically should that be temporary.
It can be extended to encompass zero trusts main directive of "never trust, always validate" even if the user was previously authenticated on to the network environment – this allows an administrator to impose a different authentication method.

Whilst this can naturally impede a user in their day-to-day duties and drive them to replicate credentials (which is never a good thing), technology has intervened to allow the implementation of simpler access procedures to reduce user drag when accessing any system regardless of criticality.

NCSC CAF states when accessing an essential function, there are three outcomes that must be achieved.

a) Identity Verification, Authentication and Authorisation – that you do it and do it well
b) Device Management – that you have trust in the devices used to access systems.
c) Privileged User Management – that you add additional management rigour to apply enhanced access

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

So why is the Identity and Access Control principle important

THE AIRPORT SCENARIO

So, think back to summer (how long ago does that feel now?) when you left these shores to go somewhere that hadn't turned the heating off.
Maybe a family member gave you a lift and helped you into the airport, they could walk into the check in area unimpeded and access the (somewhat scant) retail outlets and check in desks without showing identity credentials [guest access].

The first challenge is at the check in desk (check in can now be done in advance but if you are carrying luggage for the hold this has to be dropped) you pass your credentials [identity validation, device trust], they are validated, and your hold bag (payload) is scanned to ensure it is not dangerous.

At this point you say goodbye to the family member that bought you to the airport as they don't have the necessary permission to go to the next stage [rejection of user without credentials].

The security hall – everyone's favourite! Forget the large queues and the man next to you with Halitosis for a minute (difficult I know), this bit is a second stage scan using technology [device trust] to scan you personally and your carry-on luggage. This reduces the risk of disruption to the airport and keeps the bad stuff away from the plane.

Once you're through the security guys, it's on to passport control [identity validation, device trust, access permission], this is another more in-depth identity validation that also checks for permissions and uses intelligence to ensure you are allowed to travel to your destination country.
This check can be more rigorous dependant on the country that issued your credentials [device trust].

Ok so you've made it to the departure lounge, it's busy and there are no relaxing areas free, but you look around and see a room that looks lovely, has lots of space and free food! The first-class lounge, there is someone on the door and they look serious. You go to the person on the door, and they ask you for ticket [privileged user management] – this is where your first-class elevated privileges come in and if you are lucky enough to have a first-class ticket, bingo the world and that very expensive malt whisky is yours.

I think you should have got the point by now. This describes identity access control in a physical example, in the digital world, like the physical, technology is added to reduce user fatigue. I'll leave it to you to decide whether it works at an airport.
I think the point on importance is made too. It is clear why you put up with the procedures you undergo on your way through an airport, why should the journey through your digital environment be any different?

Clearly sometimes these controls fail, in the airport scenario, there are documented cases where they do – it's likely they could in your digital world but there are other controls within CAF that should be implemented and tested to make sure, they catch incidents where authentication controls fail.

Things to consider

IT performance and security make uncomfortable bedfellows sometimes, traditionally convoluted access policies created a lot of the friction between the two functions, applying security controls at the expense of user experience and the inertia it caused was a problem.
This is an area, however where technology has really helped, single sign on, MFA etc make tricky access procedures simple and reduce the amount of frustration when accessing systems critical to the user's role.
Technology is not infallible though and human administrative error and poor policy decisions can still create gaps for compromise.

Considerations:

1. User roles and therefore permissions are fluid and require robust processes and procedures to manage effectively, this makes joiners, movers and leavers tracking essential.
2. Identity mechanisms can still be socially engineered, additional controls still need to be robust – it's not a silver bullet.
3. Introducing technology to support identity access control provides an increased risk from access software, systems and tooling that need to be maintained and administered properly.
4. If you don't have your critical systems and data mapped and therefore appropriate access defined it becomes pointless.

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.