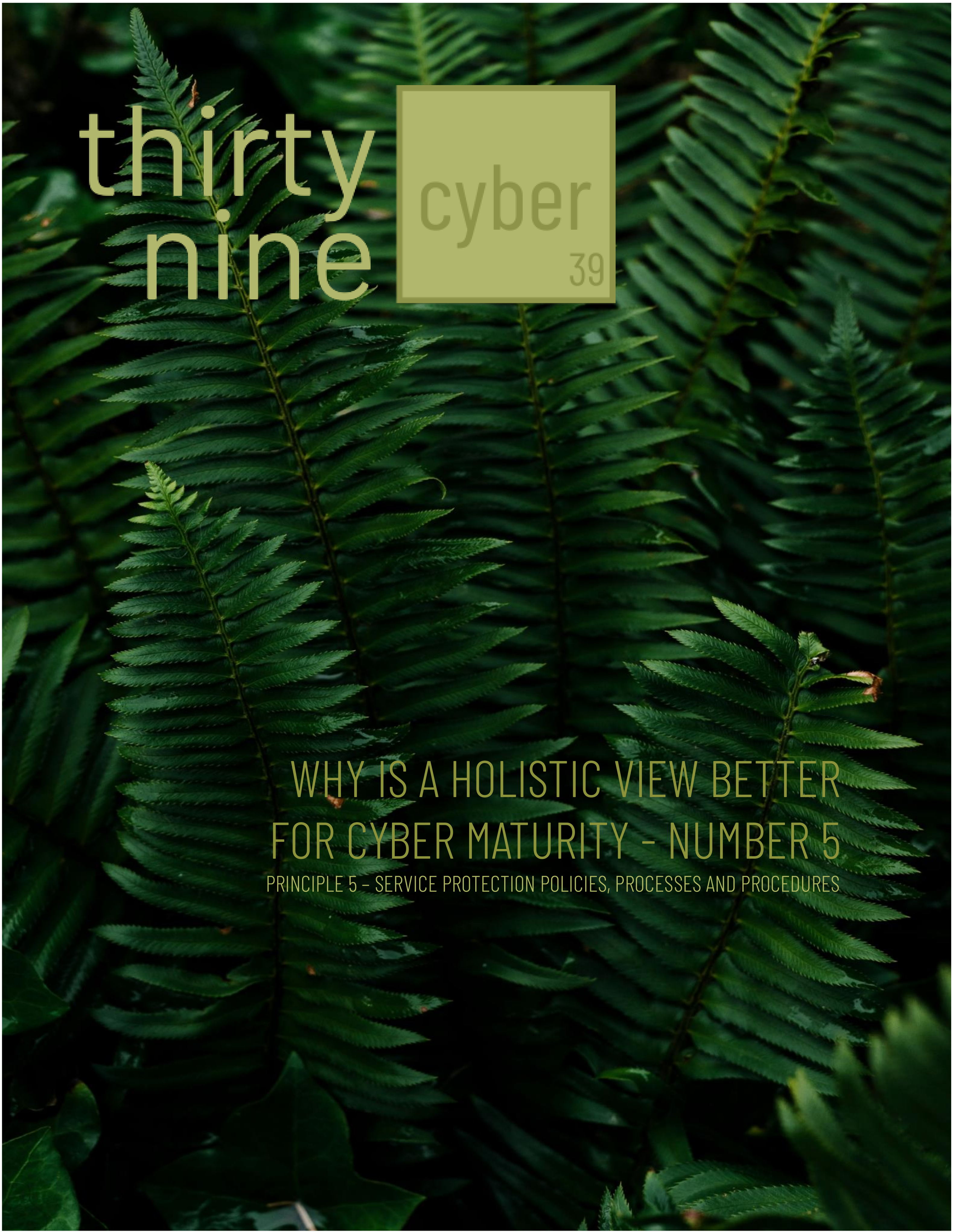
thirty nine cyber 39



WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 5

PRINCIPLE 5 – SERVICE PROTECTION POLICIES, PROCESSES AND PROCEDURES

To the reader,

Welcome to my opinion – This is the fifth one in the series – covering the fifth principle in NCSC's CAF framework – Service Protection Policies, Processes & Procedures.
Note: 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 [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. What is policy, process and procedure?
2. Why creation of poor policy or process has a flow down impact?
3. Considerations when creating, changing or implementing policy, process and procedures

Still fancy reading it?

Ok, strap in.

Service Protection Policies, Processes & Procedures

So, let's all have a bit of an eye roll to get it out of the way…
Done? Awesome!

This is one of those things that isn't sexy. It doesn't gain huge applause for tackling but is so vital that it needs proper thought and implementation.
Also, a friend of mine once said to me that if you think cyber security is sexy, you're doing it wrong, so big up for the unsexy heroes among us (that includes me by the way – well, at least the unsexy bit).

So why is the Service Protection Policies, Processes & Procedures principle important?

Policies, Processes & Procedures are the foundation of service resilience, done well they also save money and resource, they make your organisation more effective and create repeatable best practices that can be measured and enforced.

That statement alone tells you why this is important, so let's get into each element, because this is a sprawling topic

Policies – the Guvnor
The bit that tells you what resources should do and makes for a bad day at the office if they don't.

Every organisation has a set of policies, written, adopted or pursued by its employed resources (that's people and entities) or at least it should, but it's crazy how many organisations haven't done this bit flawlessly.

IMPORTANT: Cyber policies should align with the organisation's broader goals and business model, ensuring that security measures do not inhibit business critical operations or growth.

Production – there are a few ways this is done but as the author is probably human and humans tend to the path of least resistance, this could be copied from other organisation or dragged from the internet.

As making sure your policies fit your business goals and model is key, don't publish something that won't, or you can't enforce just because you think it must be included because another business had it in theirs.
It needs to be right for your business because you are going to build out processes and procedures based on this policy, and you are going to ask your resources to adhere to it.
Remember: Cyber policies must comply with relevant laws and regulations, don't forget this bit.

Adoption – if the policy relates to employee behaviour, and links to a process, don't just hand it to someone for a signature or worse upload to SharePoint and leave it to be found when policy is breached and think "policy adopted", it's not.
Take the time to explain it, and even train your people on it to ensure they understand why it's important and what the impact is of not adhering to the policy.
If the policy relates to a system or entity, ensure and review policy implementation to make sure it has been carried out effectively (this is why asset management is important).

Review – I think this is the most important bit, not that the other bits aren't important, but policies can go quickly out of date and should be regularly reviewed, as a cyber sort of guy I would say inline with threat intelligence (and that's not just cyber threat that's any change driven by external forces).

Processes – the Man with The Plan

The bit that tells you what steps need to be taken in line with the policy.

I think it's self-explanatory that processes need to clearly follow the policy that demand them, what less clear is how to do that whilst ensuring that the process is proportionate, relevant, deliverable and simple enough to work consistently and intuitively for the entity that is following the process.

If part of the process is hard or complex, automation should be considered to remove adoption issues and reduce the chance of process failure.

Any process should be tested and/or challenged before implementation to make sure that there are no nasty implications of enforcing it.

For example. if your policy says that a patch should be applied to maintain currency and security of an entity, and you define a process that says that upon release the patch should be applied, then you are wholly reliant on the integrity of the patch and trust (that's a big word here) that the patch author has tested the patch appropriate to your organisation, don't, they can't.

Patching is important but should you test it in your environment first? Should you even implement the latest version (maybe n-1 is the best way)? I am not sanctioning either but if you automated this process without testing and you wake up to a world of pain on a Monday morning then the process has failed. You may think this is not your fault, but is it?

That's easy for me to say in hindsight, harder to predict and create a process to avoid it. Hence clever people that challenge any process and lessons learned fed into any creation or change is probably a good idea.

Procedures – the Fixer

The bit that tells you how to do the steps the process defines.

Ok you wrote a policy and defined and tested a process to enforce the policy, the next bit tackles how the steps in the process are prosecuted – how do you do what the process asks you to do?
This gets confused with process... A lot!

Procedures when well written and adopted should take away the abstraction of process delivering a clear manual of how to do something within the capability of the entity.

Doing this reduces the chance of inconsistency and ensures greater efficiency and contains the cost of error and wasteful practice – IF well written and implemented, if not I can hamstring your organisation or delay outcomes so clearly its important to get right.

Policies, process and procedures should be seen as an interconnected chain that works best when created holistically and not individually.

Things to consider

This document is a toe dip into this side of cyber (or more broadly, business function).
There are some things that need to be considered but my advice is that if Policy is wrong or irrelevant, that issue will flow through the chain. If process is wrong, then procedures become difficult and expensive.

Considerations:

1. When creating or reviewing policies, don't just copy from another organisation, it's your business model this is supporting, be mindful of the capability of the entity that the policy is written for and make the policy relevant to it – if you think that security or regulation is compromised because the policy isn't robust enough because of limitations in the capability of the policy subject, increase the capability, don't try to treat with policy, it's not there to reduce the risk of a capability gap.
2. Policy adoption is critical, it should flow into process and procedures and should be exposed to ensure visibility and understanding, take onboard lessons learned to improve it, don't see it as a static position.
3. Management of Policy is critical, ensure it is reviewed (audited) regularly, any change, apply point 2. Also, each policy needs an owner.
4. Process should align to policy completely and should support the desired outcome of it.
5. Make processes intuitive and simple to enact, complex processes drive convoluted procedures that will slow your organisation down and increase operational costs and resource levels.
6. Procedure should cater for the lowest common denominator so should be simple to prosecute, its not big or clever to foster complexity.
7. Automation can be a good thing but treat it as any other resource, keep it straightforward and have clear input and output demands – test it challenge it and make sure its watertight or you will create a cottage industry in automation management.
8. Oh, did I mention, review regularly (I did BTW but I am saying it again)?
9. You will want policy, process and procedural breach to be detected and implication of it, enforceable, therefore it needs to be implemented unambiguously.

Policy, process and procedure flows into the tools you adopt, the skills you require and the outcomes you achieve, if this bit is strong, you can demand greater reduction in risk.

Balance the costs of implementing policy, process and procedures with the potential financial, reputational, and operational risks of not having adequate protection.

Once in place you can ensure policies are consistently enforced through technological controls, management oversight, and employee accountability.

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.