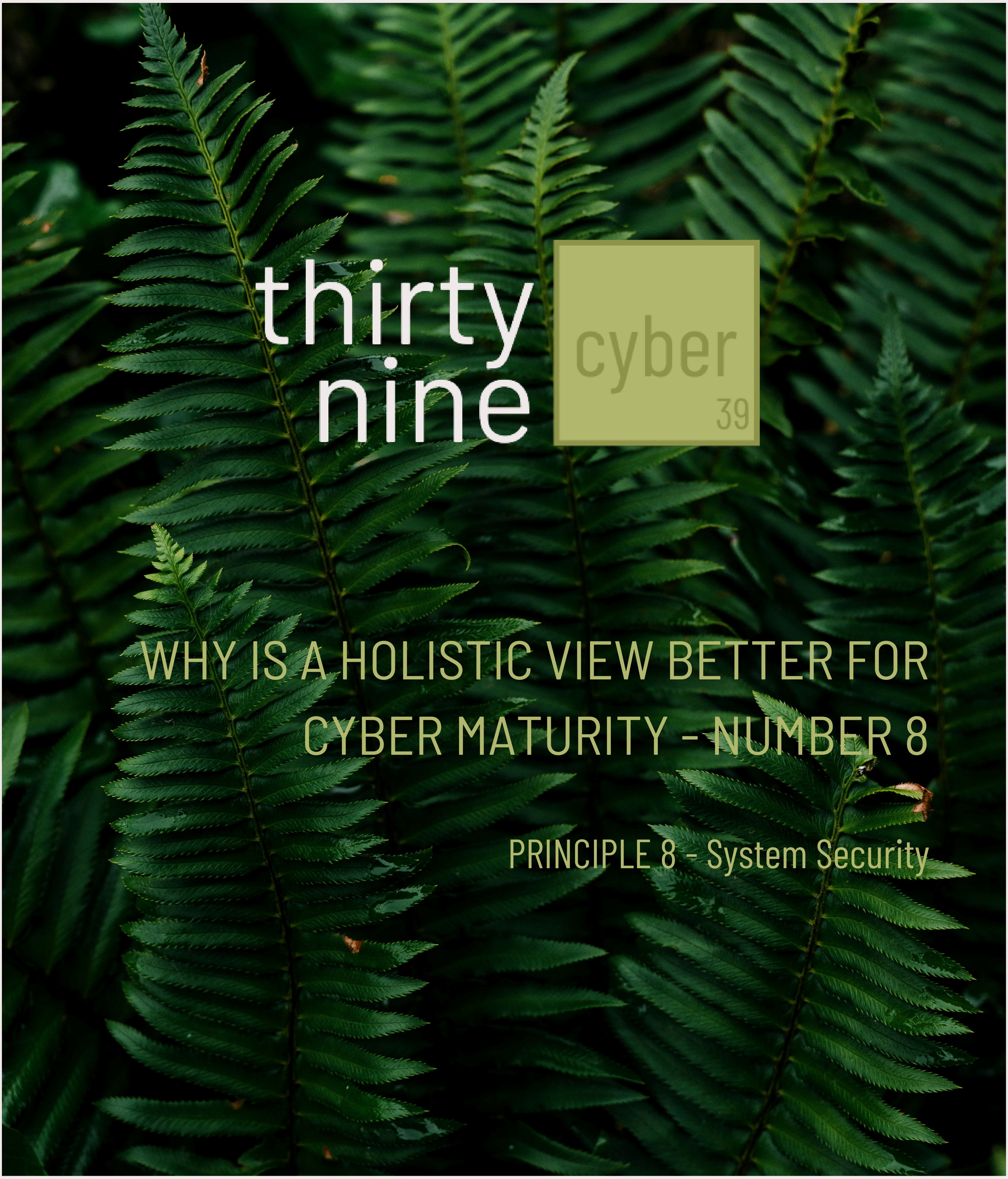


thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 8

PRINCIPLE 8 - System Security

thirty nine cyber 39

ASSESS. ADDRESS. SUCCESS.

Enabling You to Make the Right Decisions About Your Security.

STUART.AVERY@THIRTYNINECYBER.COM

To the reader

Welcome to my opinion – This is the eighth one in the series – covering the eighth principle in NCSC's CAF framework – System Security.
Note: I really only tackle the first steps here, more to take you the reader back to the fundamental point. 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. Questions you should ask of your systems and system administrators to define criticality
2. Some tips as to how to approach the principle, the board and risk mitigation

Still fancy reading it?

Ok, strap in.

System Security

I think it's at this point in the series where the framework really demonstrates the interdependent nature of security, a lot of what I say here will sound like replication from before but there are important nuances, it's progression rather than duplication. It's important that both the assessor and the assessed understand these nuances as there may be a tendency for those not familiar with the framework to skip important points of difference.
Systems, critical to the operation of your organisation are important, Yeah, I didn't really need to say that, but I will say it anyway.

There is a point though, when approaching this principle, it is important to understand what your critical systems are and there are questions you should ask:

- What does the system do? Or more specifically, what specific operations, processes or functions rely on this system?
- What other systems, processes or people rely on the operation of this system, are there upstream or downstream systems that would be impacted if the system failed?
- If the system failed, how long could the operation continue without it (if at all)?
- What consequences (financial, reputational or legal) would arise from a failure?

The potential impact of a system failure gives direct insight into its criticality. Systems that, if unavailable, could impact operations, cause significant revenue loss, or lead to legal consequences are probably critical.

Ask the questions and categorise the systems criticality i.e.
Mission-critical: If this system goes down, the entire operation stops.
High: The system is important; its failure would result in limited or temporary disruption.
Moderate: The system's failure would cause inconvenience but wouldn't have significant operational or financial consequences.
Low: The system supports non-essential tasks that don't impact overall operations significantly.

With this categorisation you can assess system security relevant to the criticality of the system, CAF focusses on assessing the systems that form part of your organisations critical function, so consider the Mission Critical and High Criticality first, it will save you time and add perspective.

NCSC CAF states that to secure systems, there are four outcomes that must be achieved.

- Secure by Design – You design security into the network and information systems that support the operation of your essential function(s) and reduce its attack surface.

- Secure Configuration – You securely configure the system, document, patch, maintain and manage change with security in mind
- Secure Management – you ensure only those you trust administer the system and retain technical knowledge (documentation) to ensure no reduction in administration capability over time.
- Vulnerability Management – You actively test for vulnerabilities and check and mitigate "announced" vulnerabilities in the systems software, firmware and hardware.

Given that this is a cottage industry in itself, it helps to be able to prioritise the most critical to your operation.

Why is the System Security principle important?

Do we need to dwell here?

Imagine – you wake up to find your customer facing service is down due to a compromise – it's offline and you can't access it…
I can stop there, right?

Things to consider

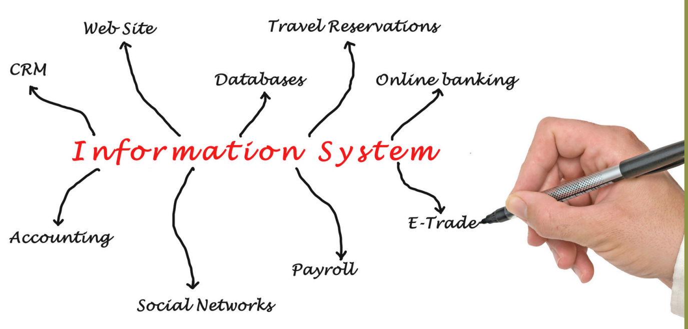
There are some considerations to make when approaching system security, I spell out some here but this is the CISO's home territory and should be second nature.

Considerations:

We've covered the first thing to consider above, but I am going to repeat it because it's important.

1. Conduct an inventory of systems and classify them based on their criticality to your operation – IMPORTANT TO NOTE: the systems your operation relies on may not be operated by you, if you have outsourced it's operation you will need to involve the third party that is (we talked about third party management in part 4, maybe have a read to see what other measures need to be considered there). Remember if the Mission Critical system relies on another system, that system becomes Mission Critical
2. Consider how you present system criticality to the board, my advice is to make risk of disruption and BUSINESS impact clear. You can use Business Impact Analysis to do this, they should be familiar with the techniques, and it will spell out the impact of system disruption in a way they understand but be careful of becoming to sensationalist (or appearing to be) no one wants to be Chicken Licken (you might need to look that one up before that reference lands).
3. The first two spell out the impact but to quantify risk you need to gauge probability, threat and vulnerability assessments will help you here – reducing probability is your risk lever, your focus for mitigation and will help you define your security objectives.
4. You have your security objectives, this next bit is important because now you will want to meet those objectives and that's going to take resource, that's going to cost. Gaining board trust and sponsorship and the resulting budget is therefore critical – At this point I can only go on what has worked for me in the past, so here is my view for what it's worth
    - Create a programme to mitigate the risk – this should show how budget will be assigned and the benefits of each stream – that's important, the board may feel better about releasing budget if it's in stages.
    - Make your response proportionate, make the ask fit the risk.
    - Prioritise from mission critical to low risk in order – give the board some clear benefit early in the programme.
    - Try to make the investment you are asking for align to bottom line benefit – it's the boards language.

System Security is one of the most important things to get right, to do that effectively you need to understand the systems in play and what they do for your business. The effectiveness and cost efficiency of the security controls you place and the way systems are designed are dependent on 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.