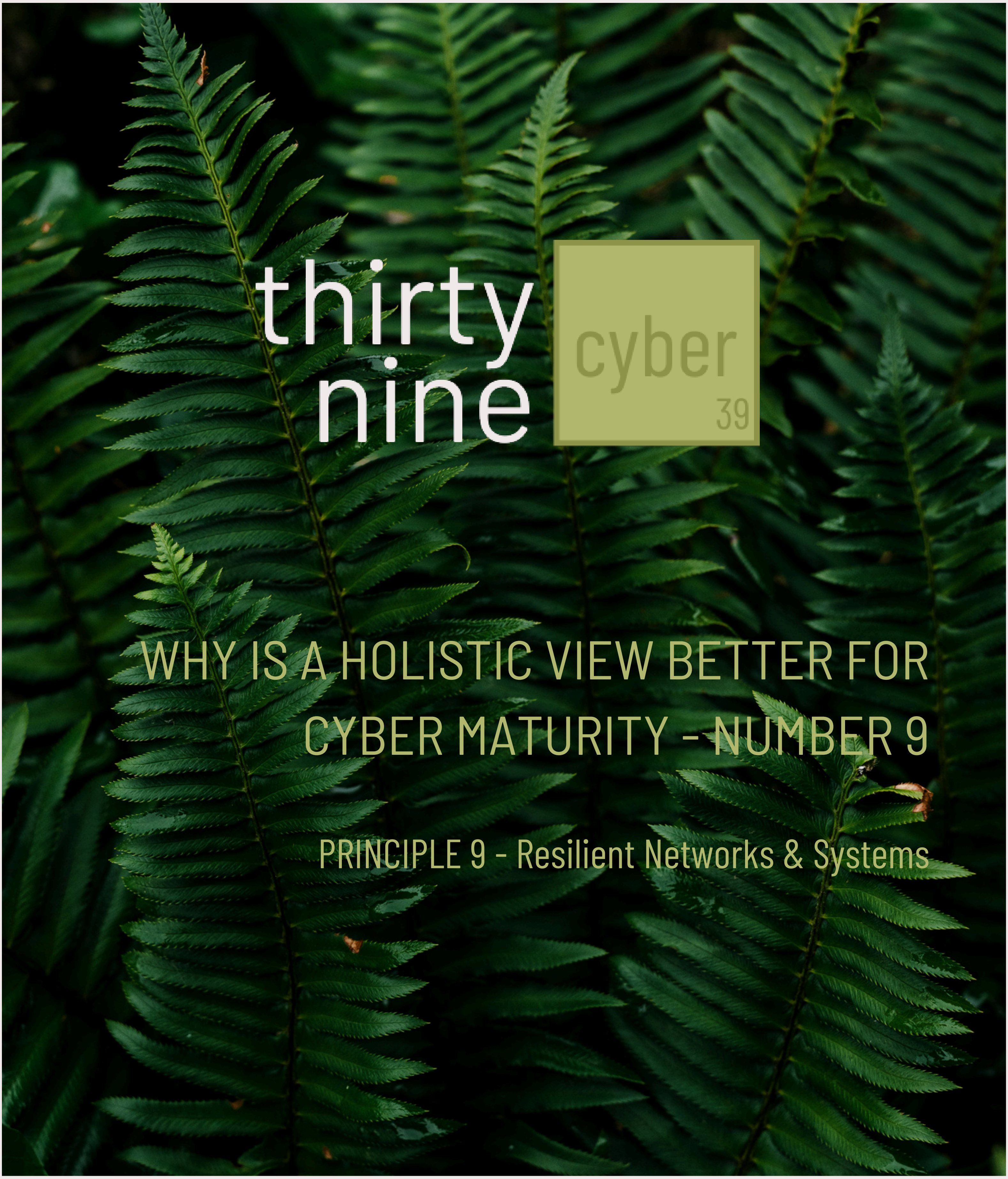

thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 9

PRINCIPLE 9 - Resilient Networks & Systems

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 – covering the ninth principle in NCSC's CAF framework – Resilient Networks & Systems.
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. Why it's important to the CEO
2. What you can do to build an effective resilience strategy.

Still fancy reading it?

Ok, strap in.

Resilient Networks & Systems

So, what does this principle tackle? well essentially, Resilient Networks and Systems is about making sure that even in the midst of an incident, your business stays up and running, and you have clear plans to recover critical systems quickly. Simple!

Key Aspects Covered:

1. Resilient Core Infrastructure: Designing the essential elements of your system so they're less likely to fail through human misadventure or attack.
2. Minimising Impact: If something goes wrong, having safeguards and comprehensive response plans in place to keep the business impact small and contained.
3. Recovering Quickly: Ensuring you have frequently tested recovery plans so that if something does fail, you can continue operations without a major meltdown.

I'll elaborate with a simple scenario:
Think of your network and systems like a well-oiled restaurant kitchen. You've got chefs (servers), waiting staff (connections), and customers (users) the chefs and waiters are working hard to get the right orders to the right tables, without burning the food or letting it go cold.
Imagine it's peak hours, and suddenly a rat (let's call it a cyber attack) is spotted the kitchen. Chaos, right? But a resilient kitchen doesn't freak out and close its doors. Instead, it has protocols. The staff have been trained and know what to do - contain the rat, sanitise the impacted areas, and keep the dishes coming so your customers aren't impacted by the incident. Make sense?

Ok so your digital environment is not a kitchen but the scenario should at least highlight what I mean by resilient.

Why is the Resilient Networks & Systems principle important?

Or rather why does it matter to a CEO

The Resilient Networks & Systems principle is essential for ensuring that your business can withstand and recover from unexpected disruptions, whether from cyber attacks, system failures, or unforeseen incidents. Here's why it's critical:

Minimising Downtime and Revenue Loss - System outages can directly impact operations, leading to lost revenue, dissatisfied customers, and reputational damage. Resilient systems are designed to maintain continuity, even during an incident, ensuring the business stays alive.
Limiting the Impact of Cyber Attacks - Cyber attacks are probable, resilient system design prioritises damage containment, attack isolation, and prevents a single incident from cascading into a full-scale business disruption.
Protecting Data Integrity and Availability - Data is one of your most valuable assets. Resilient systems ensure that your critical information remains secure and accessible, even if some components are compromised, keeping business operations stable.
Meeting Legal and Regulatory Obligations - Regulatory compliance requires that businesses maintain service integrity and protect customer data. Failing to demonstrate resilience not only risks operational setbacks but also exposes the organisation to significant legal and financial penalties.
Building Stakeholder Confidence - Your customers, partners, and investors expect reliability. Demonstrating the ability to keep services running, even under pressure, builds trust in your organisation's capacity to deliver consistently and securely.
Supporting Business Continuity and Rapid Recovery - Resilient systems are designed to recover. Rapid restoration of normal operations after disruptions minimises financial impacts and keeps the organisation trading.

In summary, resilient networks and systems are about keeping the business secure, reliable, and prepared for the unexpected - ultimately safeguarding your bottom line and your reputation.

Things to consider

There are some considerations to make when approaching the resilient networks and systems principle, I spell out some here but this isn't exhaustive. These will help you structure an effective resilience strategy

Considerations:

- What makes your business tick? Determine which systems, data, and processes are most essential to the business. These should be secured and kept operational during an incident. Ensure that resilience effort supports the overall business strategy and risk appetite. For example, if the company prioritises uptime and customer trust, resilience resource should reflect this (sometimes this is a tough message to take into a boardroom).
- Understand the risk to your critical systems. Detail the potential risks and threats, from cyber attacks to user misadventure and system failure (external threat and Internal risk). Threat modelling helps to prioritise where to allocate resources for maximum effect.
- Resilience Strategy. Have one! Establish clear objectives for resilience based on business priorities, that will sit well with senior leadership stakeholders and be holistic in your approach to alignment of objectives. Engage business units, risk management, and senior leadership.
- Technical Infrastructure and Architecture. Where necessary maybe segment the network to isolate issues and contain incident proliferation. Build in redundancy where appropriate and implement reliable backup solutions to restore lost systems quickly.
- Incident Response Planning. Have a plan. Test the plan. Make sure every stakeholder knows the plan and their role in the plan. Train the response team on the plan. Regularly review (use any lessons learned) and if necessary update the plan.
- Invest wisely. Ensure you have just enough of what you need to be resilient, no more, no less - the board will love you for that.

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.