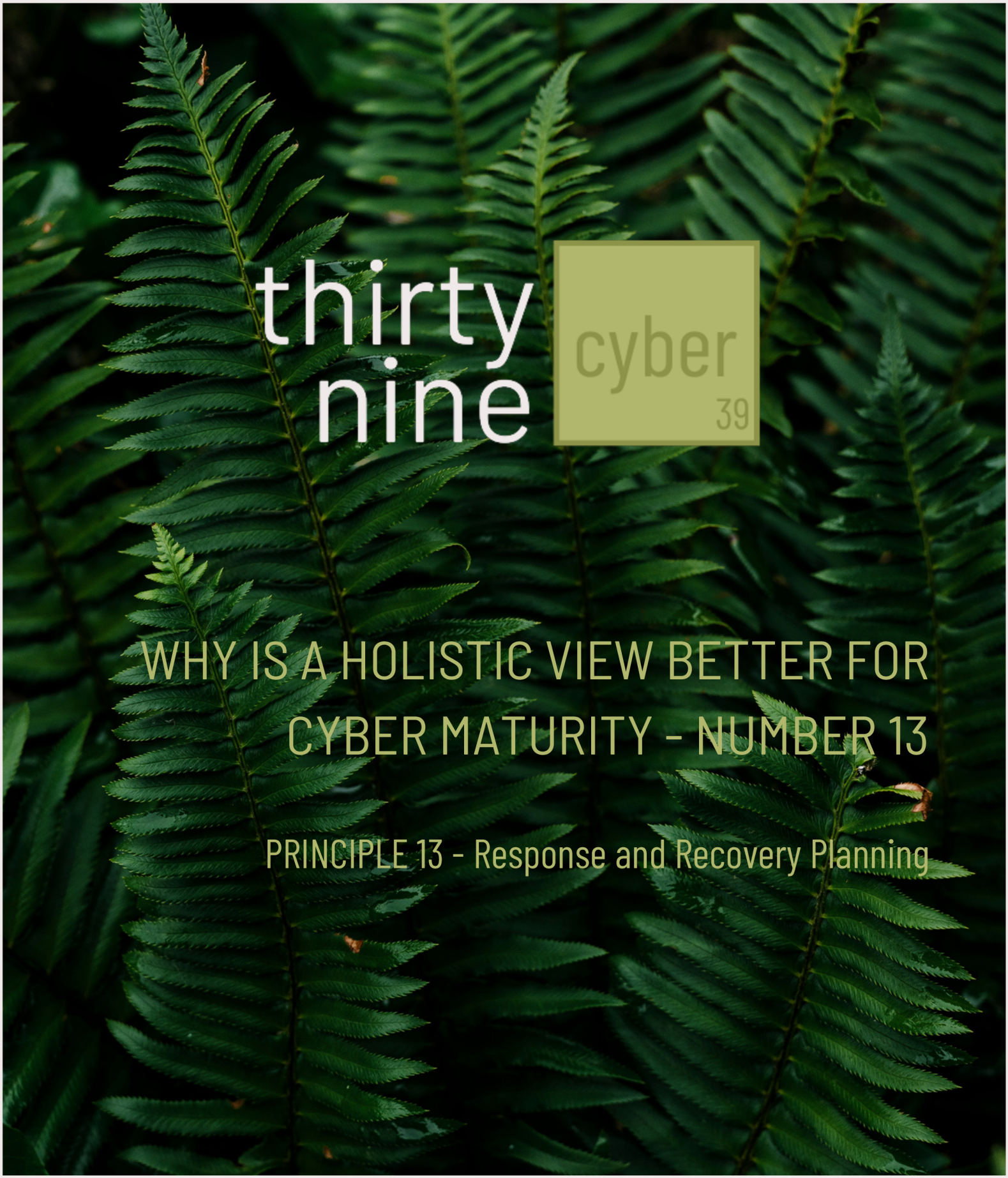

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 13

PRINCIPLE 13 - Response and Recovery Planning

thirty nine cyber 39

ASSESS. ADDRESS. SUCCESS.

Enabling You to Make the Right Decisions About Your Security.

STUART.AVERY@THIRTYNINECYBER.COM

To the reader, an introduction

Welcome to my opinion, covering the thirteenth principle in NCSC's CAF framework – Response and Recovery Planning (and testing).
For many organisations where budget and resource constraints are a factor, this principle is critical. this document walks through why that is and why focus on this principle is important.

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 so here is a summary view.

What's in it

1. Why response and recovery is NOT a vanity exercise.
2. How response and recovery planning is critical to your operational resilience and your brand.
3. What things need to be considered to help you plan and test your response to an incident.

Still fancy reading it?

Ok, Make a cup of tea, find a quiet place and read on..

Response and Recovery Planning

What is it?

CAF outlines this principle as well-defined and tested incident management processes, that aim to ensure continuity of essential function(s) in the event of system or service failure.

Pretty straightforward then as a statement but a plan relies on a number of key components.

1. An understanding of the critical functions, the systems your organisation relies on to operate and the potential vulnerabilities and access points that exist that could be exploited or exposed by a malicious actor or by user misadventure.
2. An appreciation of the potential threat to those functions and the target of a potential compromise.
3. Any regulatory requirements that your organisation may be required to adhere to.
4. A well defined set of potential incident scenarios that may materialise driven from the outputs of points 1 & 2, and,
5. A defined set of stakeholders and their roles & responsibilities during an incident based on the scenarios identified.

once these are in place then you can begin to create and test plans to respond and recover from an incident effectively.

Why is the Response and Recovery Planning principle important?

All good security strategies assume that a breach is inevitable, It's ok to hope for the best but you should plan for the worst.

Here's why it's important:

Response and recovery planning is a cornerstone of good cyber resilience. It's not a vanity function; it's about being prepared, the best defences can't guarantee total immunity from incidents, so knowing how to respond and recover quickly and effectively can make the difference between a minor hitch and a business-critical event.

Of course having the plan is only any good if you know it works, you need to ensure the stakeholders listed in the plan have visibility of the plan and ensure they understand their role and its good practice to practice, exercises to ensure that the plan is robust, complete and actionable are probably a good idea.

Don't do this and you are leaving your response to chance and in the heat of an incident, there's no room to find out elements within the plan don't work or create inertia.

Reasons why it matters:

1. Minimise Downtime

When an incident occurs, you may experience operational disruption, every second of downtime can cost your organisation money or harm your reputation. Having a solid response and recovery plan means you can act quickly to contain the impact and get back to business as usual as quickly as possible.

2. Protect and Even Enhance Your Reputation

A well-handled incident can actually increase trust with your customers and stakeholders. Demonstrating that you've planned for disruptions and know how to deal with them professionally can be a positive PR story. Fumbling through a crisis can damage relationships beyond repair.

3. Meet Regulatory Compliance

Many sectors now require evidence of robust incident response and recovery planning to meet legal or regulatory obligations.

4. Improve Resilience & Add Focus

Testing and refining your response plans regularly ensures your organisation becomes more resilient over time. Every dry run or lessons learned from real incidents strengthens your ability to handle the next challenge. A clear response plan gives everyone in your organisation a playbook to follow, ensuring the right people take the right actions at the right time.

5. Reduce Financial Impact

Incidents can be costly—not just in terms of ransom payments or remediation, but also lost revenue, compensation claims, and potential fines. A proactive plan can significantly reduce these costs by reducing the incidents blast radius and speeding up recovery.

Response and Recovery Planning ensures that, while you can't prevent every incident, you can control how your organisation reacts to it.

Things to consider

When approaching response and recovery planning there are a few things to consider, some are listed here, this may not be everything but it's a decent start

Considerations:

- Understand what threats you are likely to face. Think about how those threats might materialise and the risk it presents to your business, add some context, if the threat, when it materialises, has no impact, deprioritise that one over one that does. Do the same with likelihood of occurrence, this will help you define the scenarios you might want to plan for, remember this includes 3rd party.
- Develop clear response & recovery objectives. Whilst this one feels a little obscure, it's actually important, for example, if a critical function is taken down during the incident, your objective will be to bring it back into service quickly. What level of service and how quickly are therefore important factors, define those measures (RTP/RPO) as it will steer the response & recovery methodology and therefore the plan.
- Roles & Responsibilities. You will need a response team, and you need to decide who is on it and what their role is. The team need to know too, it needs to be clear what is expected of them, Roles might include, incident handlers, IT specialists, communication leads, senior representation and even legal advisors. 3rd party suppliers may need to be involved and communicated with so include them.
- If you have a SOC function. However you have implemented this, insourced or outsourced, it should provide your early stage response and therefore should be part of the broader response plan it's also the function that detects the incident in the first place and therefore should carry the playbooks to initiate the right response process. this early stage response should be defined as part of the exercise and tested, purple teaming is your friend here.
- Test & Exercise. Test, test, test, you need to make sure what you have planned works. Table tops exercises will refine the plan and increase accuracy, once you have done this use recovery exercises and red/purple teaming to test scenarios and practice response. take the lessons you learn to improve the plan.
- Business considerations. Assign a budget or resource allocation for response. Assess insurance coverage. Integrate cyber incident response into the wider business continuity plan. Understand your regulatory obligations, ensure they are considered in the plan.

Ok so I hope that all made sense, if you agree or disagree, 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.