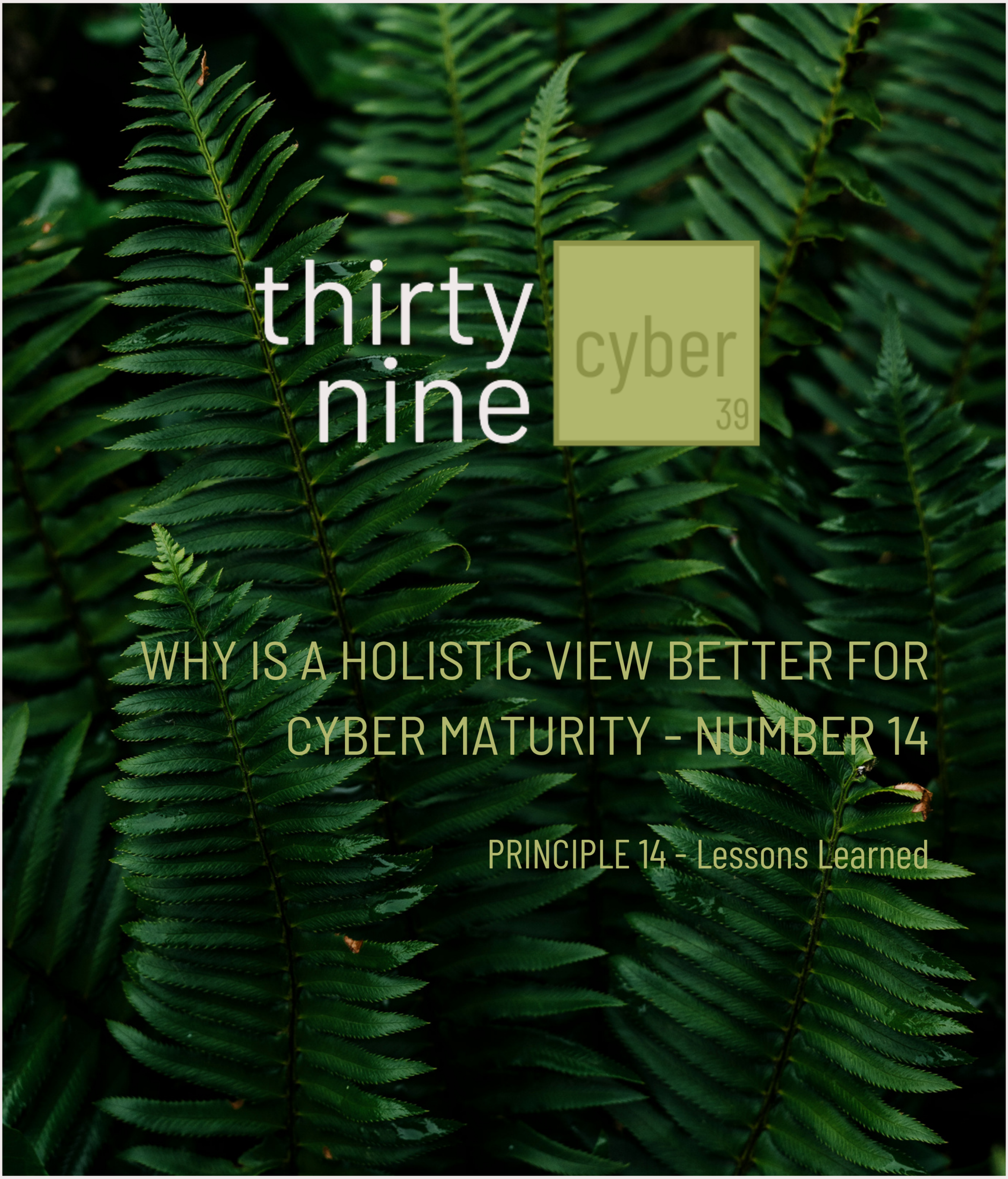

thirty nine cyber 39

WHY IS A HOLISTIC VIEW BETTER FOR CYBER MATURITY - NUMBER 14

PRINCIPLE 14 - Lessons Learned

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 – this is the fourteenth and final blog in the series covering the last principle in NCSC's CAF framework – Lessons Learned.
If you've made it this far, well done! Either you're genuinely interested in cyber security maturity, or you've got a stubborn streak that refuses to leave things unfinished. Either way, I respect it.

So here we go...

Key takeaways [TL; DR]

Because I know you're busy, here's what this blog covers:

1. The art of learning from mistakes – why post-incident reviews matter.
2. How to implement structured learning – because "winging it" isn't a strategy.
3. Turning lessons into action – making sure improvements actually happen.

Still fancy reading it?

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

Lessons Learned

What is it?

So, what's this one about? Simple: it's about not making the same mistake twice. Or, to put it another way, taking a structured approach to reviewing incidents and using those insights to strengthen your security posture.

It's a crucial part of cyber resilience and, frankly, the bit most organisations ignore because, well... it's not exciting. But ignoring it is like refusing to read the manual before and even assembling IKEA furniture – sure, you might get lucky, but sooner or later, that wobbly shelf is going to come crashing down.

Why is the Response and Recovery Planning principle important?

Why would anyone make a mistake that had a significant impact and then not try to understand what when wrong and put things in place to avoid making the same mistake again.

Here's why it's important:

Let's be honest. No one wants a cyber incident, but when one happens, it's a golden opportunity to improve. The problem? Most organisations either:

- Panic and fix the immediate issue without thinking about how to stop it happening again, or
- Conduct a lengthy post-mortem, write a detailed report, and then... do absolutely nothing with it.

Lessons Learned is about breaking that cycle. It's about turning incidents into insights and using those insights to build resilience.
NCSC's CAF framework lays this out with three core outcomes:

1. Incident Analysis – Reviewing what went wrong (without pointing fingers).
2. Learning and Improvement – Applying lessons to strengthen security.
3. Feedback Loops – Embedding continuous improvement into business as usual.

Reasons why it matters:

The pub fight scenario

Let's bring this to life with an analogy. Imagine your business is a pub. One night, a massive fight breaks out (your cyber incident).

Option A: You clean up the mess & broken glass, patch up the damage, and pretend it never happened.
Option B: You ask the staff what they saw, check the CCTV, figure out who started it, how they got in, and what led to the fight initially.
Then, based on what you've learned, you improve security, maybe:

- Training staff to spot troublemakers earlier.
- Hiring an extra doorman.
- Changing how you serve drinks to avoid escalation.

This is Lessons Learned in action. You don't just move on – you make sure next time, you're better prepared.

Things to consider

When approaching the Lessons Learned principle there are a few things to consider, some are listed here, this won't be everything but it's a decent start
So, how do you actually make Lessons Learned work?
Considerations:

- Build a culture of honest review

If post-incident reviews turn into a blame game, no one will speak up. Encourage honesty and make it safe to admit mistakes.

- Capture the right data

What actually happened? What were the warning signs? Did controls fail? If so, why? The more structured your review, the better your future defence.

- Involve the right people

Don't just leave post-incident reviews to IT or security teams. Get input from leadership, operational teams, and anyone who was affected. Cyber incidents often have business-wide implications, so insights should come from across the organisation.

- Look beyond technical failures

Incidents don't just happen because of bad tech, often it's human behaviour, poor processes, or lack of awareness that played a role.
Consider:

- Was there a missed alert or ignored warning sign?
- Did someone fail to follow process because they didn't know or found it too complex?
- Was there a communication breakdown during the response?

- Prioritise improvements

Not all lessons require massive remediation projects. Some might be simple procedural tweaks, while others might justify a bigger security investment. Prioritise based on risk and impact.

- Identify recurring patterns

If you're fixing the same issue repeatedly, you've got a bigger problem. Are there underlying weaknesses that haven't been fully addressed?

- Make it a habit

Lessons Learned isn't a one-off exercise; it should be a constant loop. Incident happens review action repeat. If you're only learning after a major breach, you're doing it wrong.

Lessons Learned is one of the most underrated but most valuable parts of cyber maturity. Organisations that take it seriously don't just recover from incidents faster, they also reduce the chances of repeat failures.
So, ask yourself: Are you learning, or just firefighting?

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.