OCTOBER 2025

CURATED

SO WHAT?

THE GOODBYE FRAMEWORK: A SMARTER WAY TO SAY HELLO TO CYBER CERTAINTY

READ ON

Introduction

Every business leader wants to sleep soundly, knowing their organisation is protected. Yet in cybersecurity, confidence doesn't come from buying the latest tech it's built through awareness, structure, and deliberate practice. That's where the GOODBYE Framework comes in.
GOODBYE doesn't mark the end of a conversation about cybersecurity it's actually where resilience begins. It stands for: GAP, ORDER, ORGANISATION, DATA, BACKUPS, YES, and EYES ON.

Each element works like a checkpoint, helping you move from uncertain to unshakeable. Leveraging the 'Keep It Simple Stupid' (KISS) principle the aim is for you to "KISS your cyber threats GOODBYE".

GAP — Where You Are vs. Where You Want to Be

Begin by identifying where you stand today. Gap analysis is about understanding current strengths and weaknesses, then targeting what makes your environment truly secure.

The first step to progress is clarity. Ask yourself:

- Where are we now, and where do we want to be?
- What do we already have in place?
- What would make us even more secure?

Your desired outcomes might include:

- Minimising financial loss
- Protecting client and company data
- Safeguarding your reputation
- Ensuring business continuity

The GAP isn't about blame it's about understanding the distance between what's current and what's possible. It's the space where improvement thrives. I bet you will find this easy right, looking internally at your organisation, how could an outside pair of eyes help?

ORDER — When the Unexpected Becomes Reality

Cybersecurity isn't just about prevention it's about preparation. So, when an attack does breach your defences, what happens next?

That's where your Incident Response Plan (IRP) comes in. This living document describes exactly what to do and who will do it when things go wrong. Indeed you may have multiple IRPs for different situations.

The purpose of the IRP is simple:

- Contain the incident quickly.
- Maintain critical functions.
- Communicate clearly (internally and externally).
- Restore operations securely.

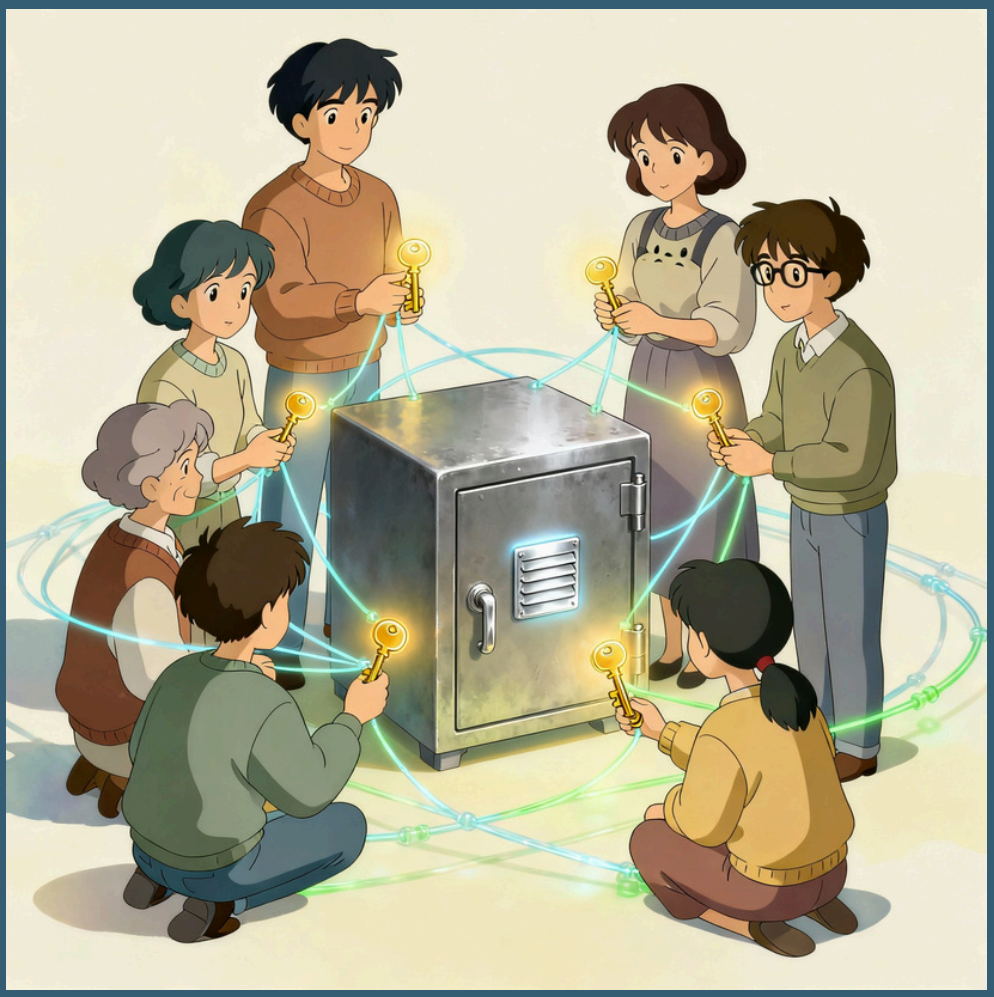
It should cover all major breach types:

- Cyber Threats: such as ransomware or phishing.
- IT-related: like failed updates or server outages.
- Physical: like theft, intrusion, or sabotage.

The right plan doesn't remove chaos; it gives chaos boundaries.

ORGANISATION – Who Holds the Keys

Every company has key stakeholders: individuals and partners whose access could make or break the organisation's safety.



Reflect on:

- Who are your critical people?
- Why are they important?
- What do they have access to and should they?

Resilience is collective. Protecting yourself means expecting accountability across your ecosystem.

Don't stop at your own team. Look into your supply chain too.

- Do suppliers have access to your data or systems?
- Have you assessed their security controls?
- What would happen if they suffered a breach?

DATA – Defending the Crown Jewels

Every organisation has something priceless its 'Crown Jewels'. For some, that's client information; for others, intellectual property, financial records, or the systems that make you exceptional.

Ask:

- What must never fall into the wrong hands?
- How do we store, encrypt, and monitor it?

Key strategies include:

- Encryption - always at rest and in transit.
- Segmentation - isolating critical data from general systems.
- Least privilege - giving users only the access they need.

Data protection isn't about paranoia it's about preserving those elements of what you do that you deem valuable, that might be; intellectual property, customer data, payment records, the systems and processes that are your 'Secret Sauce'.

BACKUPS - The Safety Net That Saves You

You can't predict every failure but you *can* plan for recovery. Backups are the unsung heroes of business continuity.

Consider:

- How frequently are backups performed?
- Are they encrypted, tested, and immutable (protected from alteration)?
- Do you follow the 3-2-1 rule , 3 copies, 2 media types, 1 offsite?
- Who has access, and is that access controlled?

Redundancy isn't waste it's resilience. Backups give you the ability to say, "We can recover." Importantly checking that the backup works on a regular basis will set you aside from many who just wait to see if it will work in an emergency.

YES - Accreditation, Assurance, and Action

You might already be accredited, insured, and training your staff, great! But compliance isn't the finish line.

Ask yourself:

- Are we spending wisely across prevention, protection, and insurance?
- Do we do what we say we do or just document that we do it?
- Are we planning toward higher accreditation, like Cyber Essentials Plus or ISO27001?

Accreditation is value multiplied by sincerity. It's only meaningful when reality mirrors the paperwork. Having the right insurance and accreditation in place will not remove cyber threats, or guarantee never suffering a successful attack. They will be part of a process that helps improve your protection and decrease the likely severity of an attack.

EYES ON - Independent Oversight

No matter how capable your internal team is, independent review keeps you sharp. Outside experts see what internal familiarity might miss. That also goes for when you have outsourced your IT.

Regular vulnerability scans, penetration tests, and external audits confirm whether your security measures truly hold up. Cyber threats evolve daily, letting someone else “mark your homework” ensures you see beyond your own blind spots. Typically business decision makers who outsource IT will be satisfied with their provider saying 'yeah we can do your cyber security'. Quis custodiet ipsos custodes?

Why GOODBYE Matters - And What's Next

Complacency is the real enemy in cybersecurity. Threats evolve, but the GOODBYE framework lets organisations keep pace by focusing on the essentials and adapting to new risks. Challenge your team to pick one step this month for fresh attention, and track progress together. If practical help, external review, or team training is needed, find the right experts that are always ready to guide your next move. Let's say GOODBYE to cyber risk for good. You can't predict every failure but you can plan for recovery.

Conclusion: Saying Goodbye to Guesswork

The GOODBYE Framework isn't about fear; it's about foresight. It doesn't end security conversations it lifts them.

When your organisation knows its GAP, defines its ORDER, understands its ORGANISATION, protects its DATA, maintains its BACKUPS, verifies its YES, and keeps EYES ON you're not just reacting to threats. You're leading with confidence.

Say goodbye to uncertainty, and hello to Cyber Certainty.

To talk to us more about how you might implement any and all of the above:

email: enquiries@incommsec.com

Jump on a quick call: https://calendly.com/mike-q/cyber-security

We look forward to talking with you.

OCTOBER 2025

CURATED

WANT TO HAVE A SAY?

ASK A QUESTION OR GET IN TOUCH

ENUIRIES@INCOMMSEC.COM