FROM DETECTION TO RESILIENCE: BEYOND THE SOC TO TRUE CRISIS READINESS

Jamie Roderick, VP Detect and Respond,
LRQA

LRQA
Your Risk Management Advantage

LEADERSHIP SERIES

01

CYBER THREAT - 2025

LEADERSHIP SERIES

HIGH-LEVEL STATEMENTS

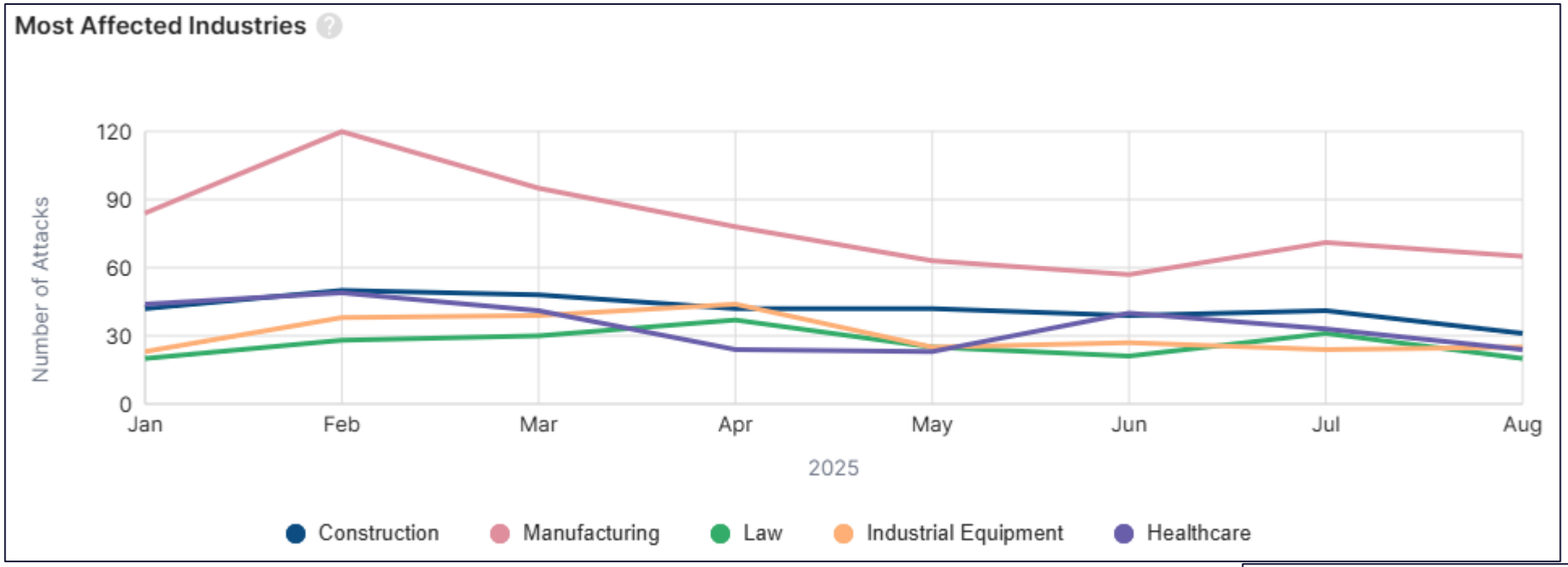
Consider the following:

22,000+ cyber attacks occur globally each day (1 every 39 seconds)	**Ransomware** accounts for 68% of detected threats, with 236M cases in 2024	Average restoration to basic service: **23 days**, full system functionality: months
Average ransom demand: **$2M**, with 94% of initial demands paid	Average cost to business **$4.88M**	Access to Encryption: 0 to 116 days • 15% encryption in one day of access • 1/3 within 48 hours of access
Phishing attacks increased by **1,265%**, driven by generative AI. 3.4Bn+ emails sent daily	Cloud intrusions increased by **75%**, with 23% due to misconfigurations	DDoS attacks rose by **31%,** with an average of **44k** attacks per day

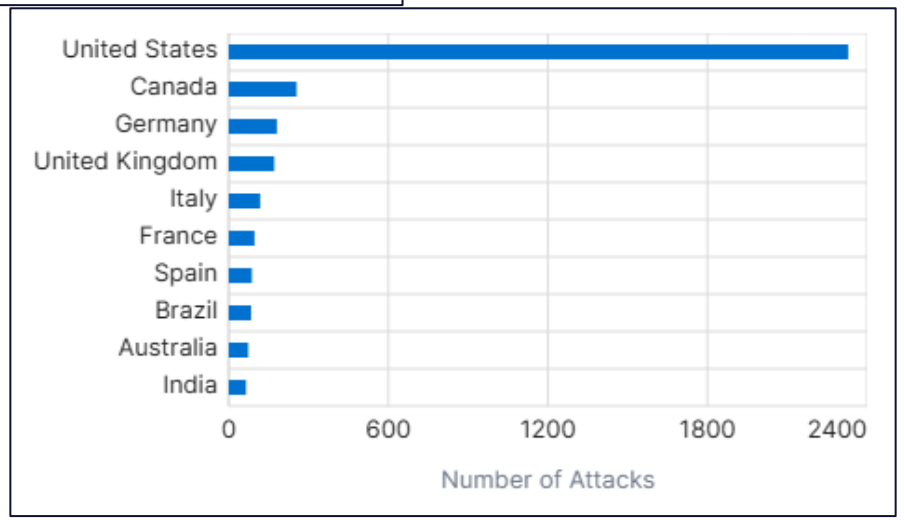
LRQA

LEADERSHIP SERIES

TOP TARGETED INDUSTRIES, SEP 24 – MAR 25

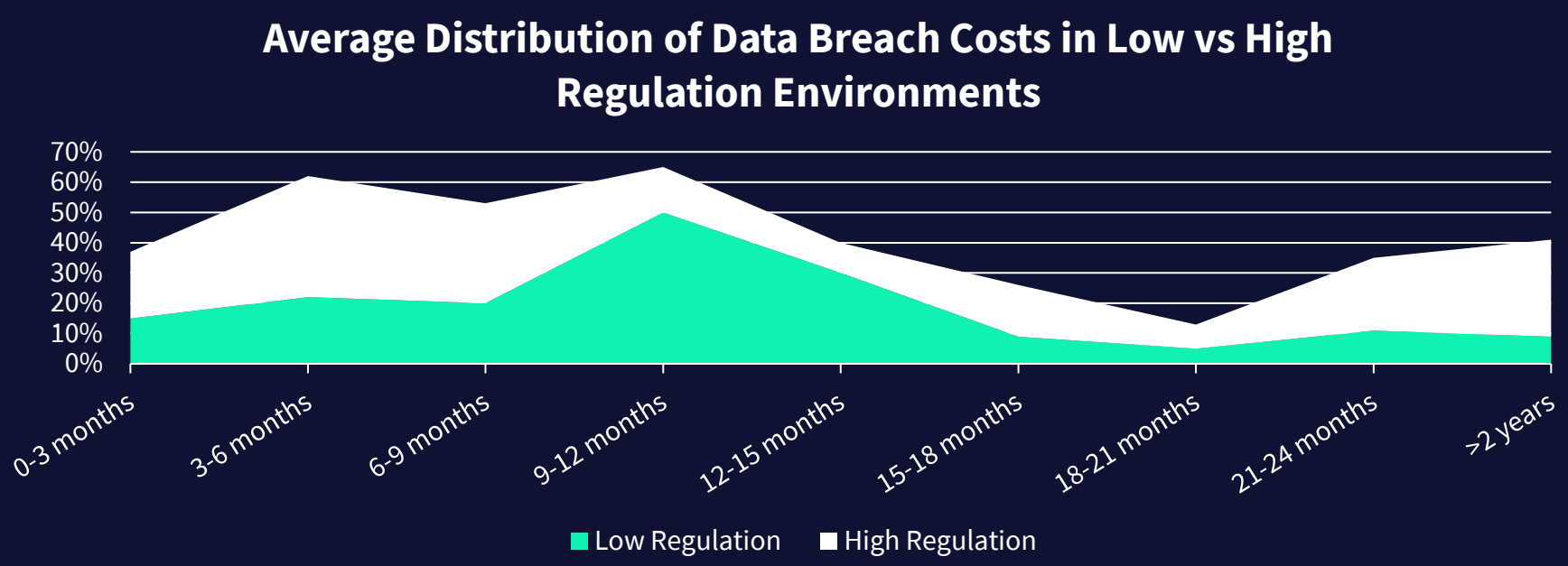


Source: Recorded Future



THREAT LANDSCAPE

How long do data breaches impact?



- Highly regulated environments incurred 45% of breach costs in the first year, 31% in the second year, and 24% more than 2 years after a breach
- Driven by new regulatory fines and the introduction of **breach notification laws**

LRQA

LEADERSHIP SERIES

02

SO YOU HAVE A SOC...

LEADERSHIP SERIES

SOC CHALLENGES

Common issues affecting SOC monitoring capabilities

Volume and velocity of alerts

- Massive data inflow from cloud, endpoints and applications
- Alert fatigue due to high false positive rate
- Difficulty in prioritising what truly matters

Complexity of modern environments

- Hybrid and Multi-Cloud architectures introduce visibility gaps
- Custom development and rapid deployment cycles outpace traditional monitoring steps
- Asset sprawl makes it hard to track what's in scope

Advanced threats and evasion techniques

- Attackers using living-off-the-land tactics, fileless malware and AI-driven obfuscation
- Threats often bypass signature-based detections and exploit behavioural blind spots

Siloed Cyber Functions

- SOCs often operate independently from IR, TI and crisis teams
- Lack of integration delays response and reduces situational awareness

LRQA

LEADERSHIP SERIES

SOC CHALLENGES

Common issues affecting SOC monitoring capabilities

Third-party (and fourth/fifth party) and supply chain risk

- SOCs may not have visibility into vendor activity or access levels
- Delegated tasks does not mean delegated responsibility – monitoring is essential

Talent shortage and burnout

- Skilled persons are in short supply and often overwhelmed
- Retention is difficult in high-pressure, reactive environments

Limited automation and AI adoption

- Many SOCs still rely on manual triage and investigation
- AI and Orchestration tools are misunderstood, under-utilised or poorly integrated

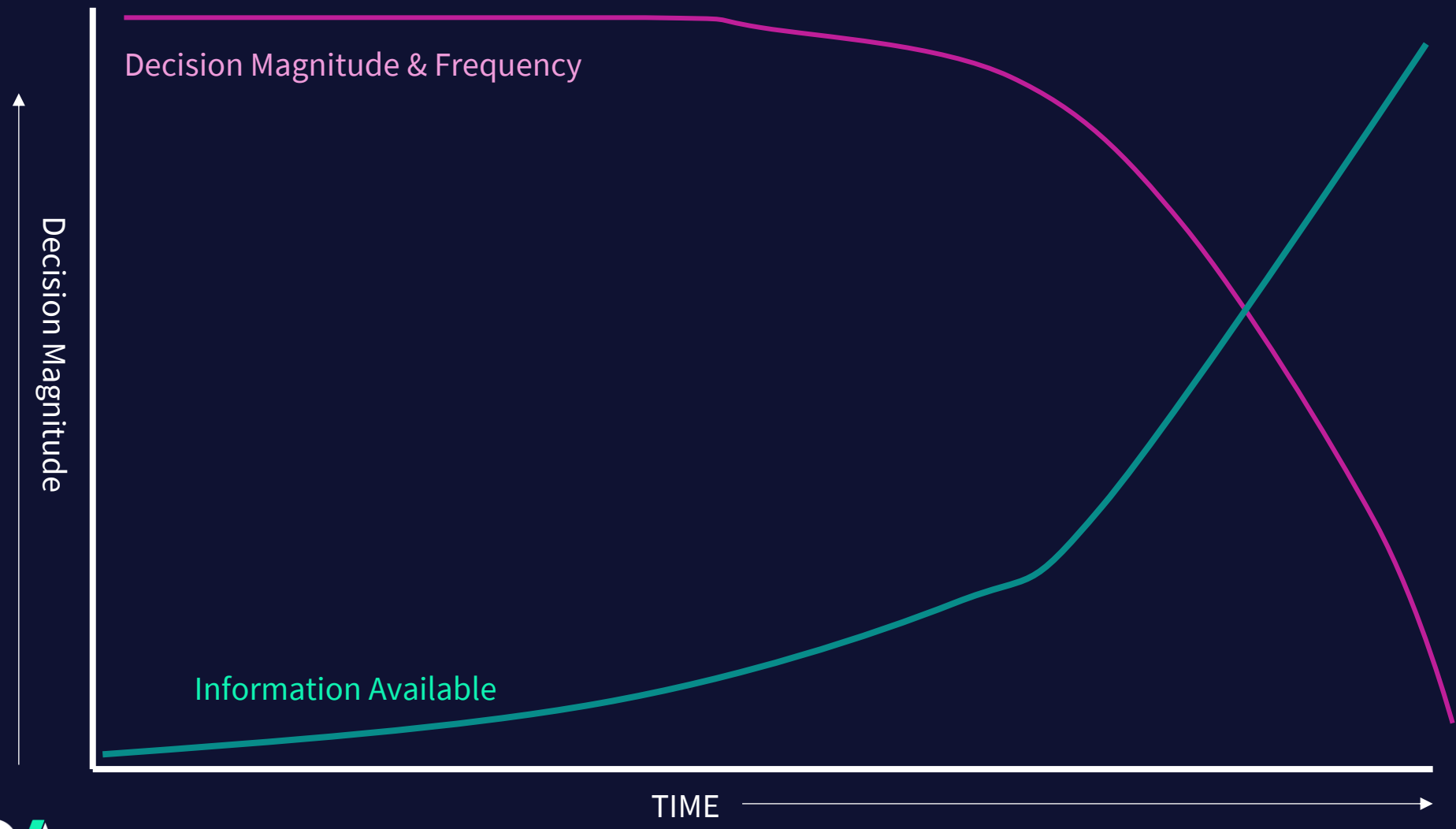
Inadequate testing and simulation

- Response plans are rarely tested in realistic multi-faceted scenarios (including technology and business elements)
- Lack of muscle memory leads to confusion during real incidents

LRQA

LEADERSHIP SERIES

DECISION MAKING IN A CRISIS



LRQA

LEADERSHIP SERIES

THE HUMAN REACTION

Fear, uncertainty and doubt

- Impacts all clients
- Natural human reaction
- You need to the right as soon as possible to enable you to make rational and risk-based decisions
- Emotive decisions are problematic
- Being comfortable with being uncomfortable
- You may not have the data to answer all questions
- Focus on impact, not the cause (at least initially)
- Cognitive bias

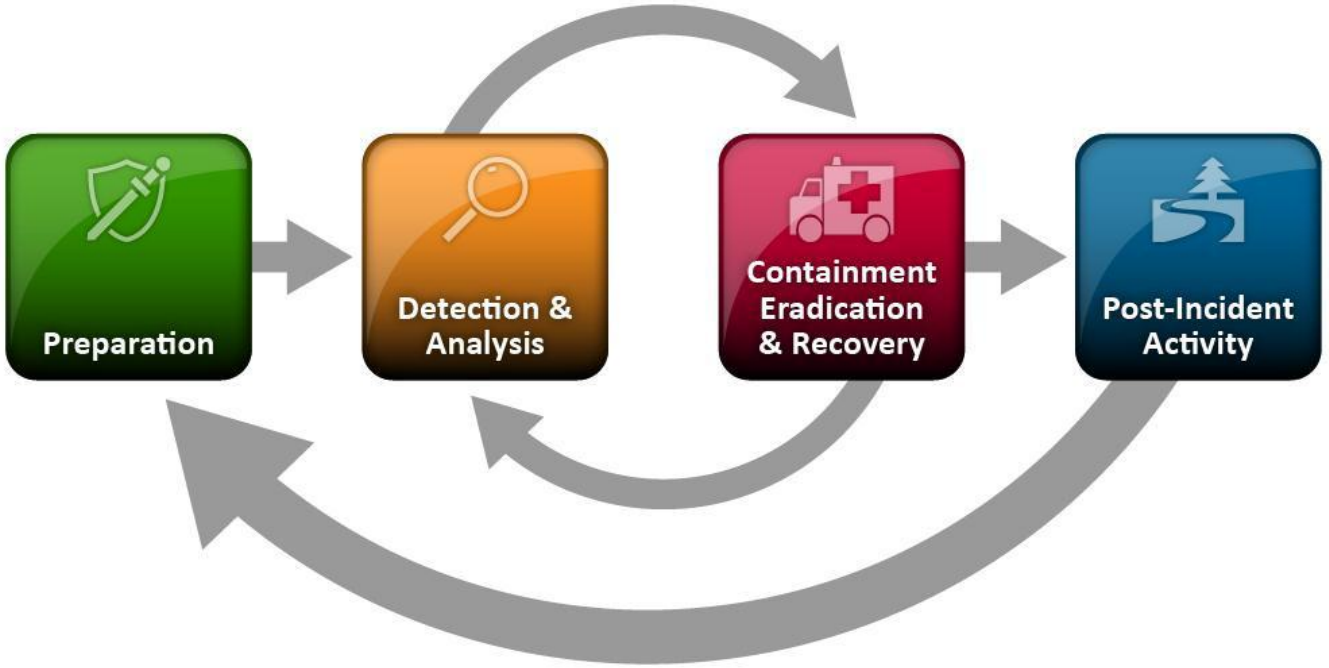
LRQA

LEADERSHIP SERIES

INCIDENT RESPONSE LIFE CYCLE (OLD VERSION)

Ransomware: requires "you to be brave and make effective and decisive isolation/shutdown decisions"

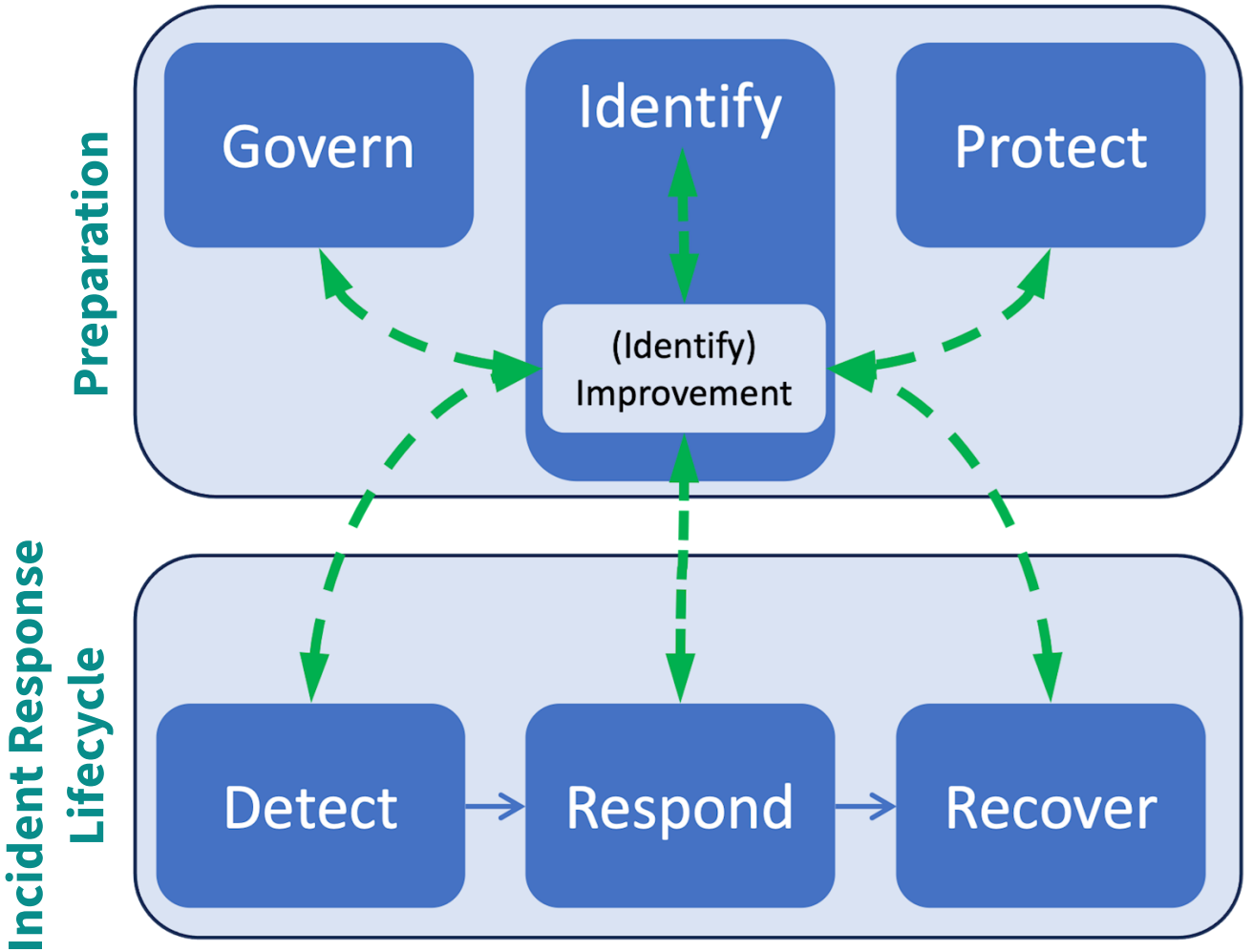
- NIST SP-800-61r2
- Steps are largely linear
- Worked quite well until…
- Ransomware, AI, Badness as a service and the related scale and complexity of attacks
- Which has led to a bit of a re-think in v3



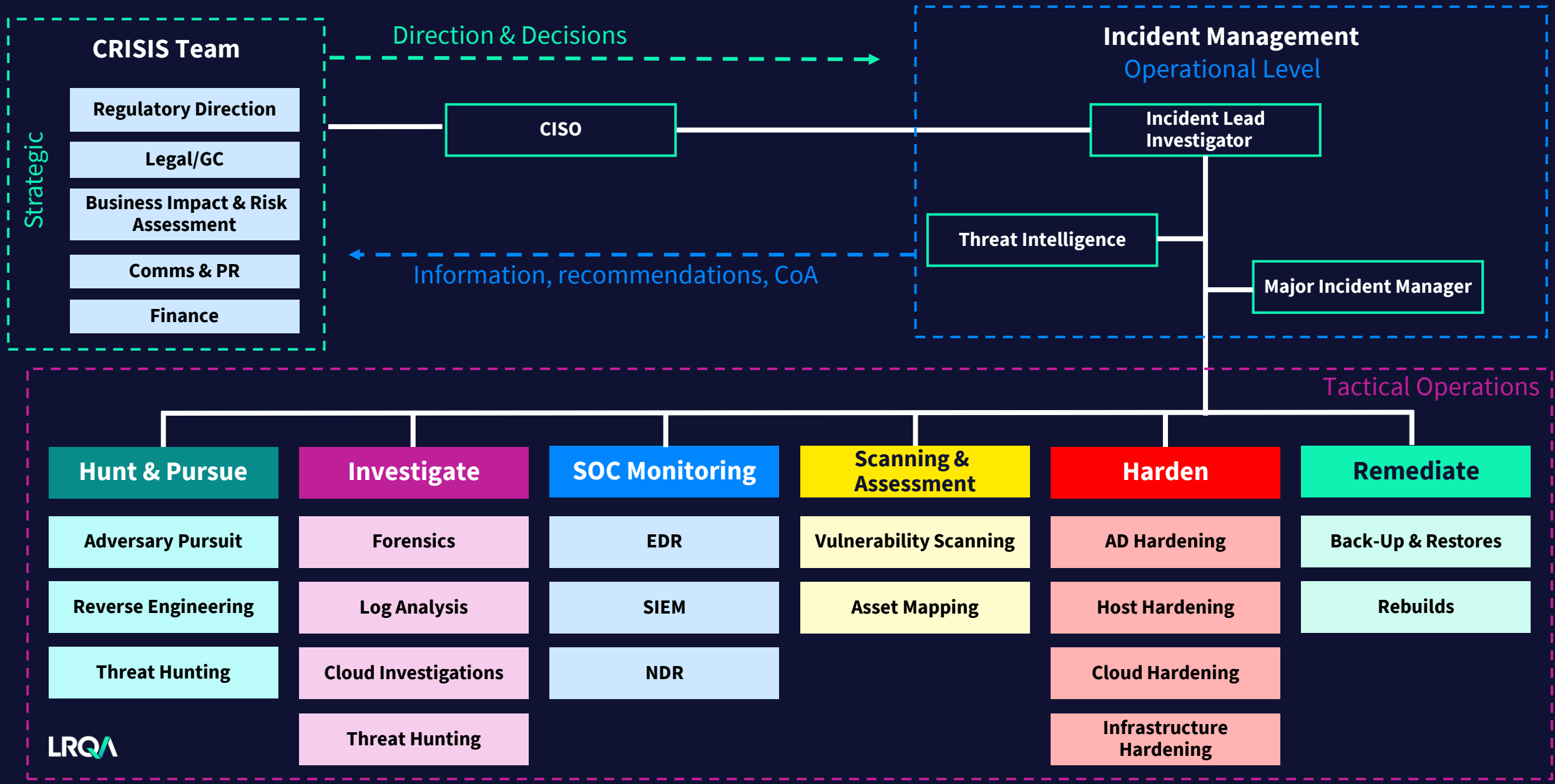
INCIDENT RESPONSE LIFE CYCLE (NEW VERSION)

Ransomware: requires "you to be brave and make effective and decisive isolation/shutdown decisions"

- NIST SP-800-61r3
- Simpler approach to enable a greater range of actions
- Based on continuous improvement
- Includes a Governance task



CYBER INCIDENT MANAGEMENT IN A CRISIS



INCIDENT EVOLUTION

Tactical functions and capabilities over incident lifecycle

LRQA

LEADERSHIP SERIES

03

THE PATH TO RESILIENCE

LEADERSHIP SERIES

HOPE IS NOT A STRATEGY

Don’t assume you won’t be attacked	Assume you will
Don’t rely on luck or obscurity	Rely on prep, visibility, and tested response
Don’t just build walls	Build systems that can take a hit and keep going

Sun Tzu Principle	Cyber Resilience Application
“Readiness to receive him”	Incident response plans, rehearsals, and simulations.
“Not on the chance of his not attacking”	Assume breach mindset; threat-informed defence.
“Made our position unassailable”	Strong baseline controls, segmentation, zero trust, and recovery capabilities.

> The art of war teaches us to rely not on the likelihood of the enemy’s not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

Sun Tzu | Ancient Chinese military strategist and author of The Art of War

LEADERSHIP SERIES

"KNOW THYSELF" (GREEK: γνῶθι σεαυτόν)

"Know thyself" is most famously associated with **Socrates**; originally one of the **Delphic maxims** inscribed at the **Temple of Apollo at Delphi**. Socrates adopted it as a philosophical cornerstone, encouraging introspection and self-awareness as the foundation of wisdom.

In cyber strategy, this principle translates into a foundational truth:

YOU CAN NOT DEFEND WHAT YOU DO NOT UNDERSTAND

LRQA

LEADERSHIP SERIES

THE IMPORTANCE OF SELF-AWARENESS AND INTELLIGENCE IN STRATEGY

Victory comes not just from strength, but from understanding:

- Your own capabilities and limitations.
- The strengths, weaknesses, and intentions of your adversary.

In a cyber resilience context, this can be applied as:

- **Know yourself →** Understand your assets, vulnerabilities, and response capabilities.
- **Know your enemy →** Understand threat actors, tactics, and emerging risks.

> If you know the enemy and know yourself, you need not fear the result of a hundred battles.

Sun Tzu | Ancient Chinese military strategist and author of The Art of War

LRQA

LEADERSHIP SERIES

6 CORE AREAS

Asset Visibility

Maintain real-time inventory of systems, data, applications and endpoints

Especially critical in cloud, hybrid and custom dev environments

1

Risk Awareness

Understand the organisation's risk appetite & threat exposure

Map vulnerabilities to business impact, not just technical severity

2

Baseline Security Posture

Know your current controls: Patching, Identity Management, Access control

Use frameworks like Cyber Essentials, or NIST CSF to benchmark

3

Operational Readiness

Know your response capabilities: IR Plans, SOC Maturity, automation & escalation paths

Test and rehearse to build confidence and muscle memory

4

3rd/4th/5th Party Dependencies

Know who has access, what they can do, and how they are monitored

Task can be out-sourced, responsibility can not.

5

Strategic Alignment

Align cyber capabilities with business priorities: Continuity, Reputation, Compliance.

Know how cyber supports resilience, not just prevention

6

LRQA

LEADERSHIP SERIES

04

IMPLEMENTING RESILIENCE

LEADERSHIP SERIES

RESILIENCE V REDUNDANCY

Resilience: the capacity to recover quickly from difficulties; toughness

- Redundancy: ***the inclusion of extra components which are not strictly necessary to functioning, in case of failure in other components***
- Resilience may include elements of redundancy
- Should be modelled against threat scenarios (most likely and most dangerous)
- Risk-based decisions should be documented
- Incident lifecycle must still be followed, even when invoking DR plans
  - Don’t recover before you know ***how*** and ***when*** they got in
  - Restoring from compromised back-ups is a key gotcha

KEY ISSUES

1

Roles and responsibilities

Key stakeholders not aware of their responsibilities, exacerbating incident through either inaction, or poor action

2

Incident response plans

Plans are not in place, not complete or not practised

Not enough resources to enact the plan (inc BC/DR)

3

False view of security posture

Great dashboard! = Great Security

Poor practices, poor training, slow/ineffective patching

Lack of verification of what should be done v what has been done

Do not know their network

LRQA

LEADERSHIP SERIES

PRACTICAL ACTIONS

Building cyber crisis muscle memory

How we operate:

Asset discovery and visibility	Continuous scanning of cloud and on-prem environments to identify new assets (and changes to existing ones)
	Automatically tagging critical systems for prioritised protection and monitoring
	Know the criticality of what you have (Business Impact Assessment) as standard
Integrated incident response	SOC Alerts trigger automated workflows that notify IR teams, isolate affected systems and initiate forensic logging
	IR, BC, and DR plans are rehearsed together to ensure seamless execution during a real event
Threat intelligence operationalisation	External threat feeds are correlated with internal telemetry to detect early indicators of compromise
	Intelligence informs patch prioritisation and containment strategies
Simulation and tabletop exercises	Regular crisis simulations involving cyber, legal, comms and business teams
	Exercises test decision-making, escalation paths and recovery speed

PRACTICAL ACTIONS

Building cyber crisis muscle memory

How we operate:

Smart patching strategy	Risk-based patching: critical assets patched first, non-critical assets monitored or contained
	Temporary isolation or service suspension used when patching isn't immediately possible or has been ineffective
Identity and access management	Role-based access controls and just-in-time provisioning reduce exposure
	Continuous monitoring of privileged accounts and third-party access
Security hygiene and baseline controls	Cyber Essentials Plus or similar frameworks implemented and maintained (security is for life, not just for audits)
	Regular audits of patching, MFA, logging and endpoint protection
Strategic alignment with business continuity	Cyber risk mapped to business impact
	Cyber teams embedded in crisis response and continuity planning
Insurance as a safety net, not a strategy	Regular crisis simulations involving cyber, legal, comms and business teams
	Exercises test decision-making, escalation paths and recovery speed

05

COMMUNICATIONS ARE KEY

LEADERSHIP SERIES

COMMON COMMUNICATION THEMES

We are investigating using NCSC accredited forensic partners…

The highly sophisticated adversary…

99.9% of access & exploit methods are not sophisticated

1

Exploited a zero day

It was a zero day 12 months ago and a patch has been available for 11 ½ months…

2

On a third-party managed system

Need to be very sure about this!

You are still responsible for actions of 3rd parties on your network

3

No customer data was exposed or compromised

Saying this without confirming it to be true, or when insufficient evidence exists to be certain

What do you say if the forensic data doesn't exist to 100% confirm that data was exfiltrated?

4

Our forensic partner confirms/ informs us..

Errrrr….no we didn't say that

Twisting and deliberate interpretation of our reporting

5

LRQA

LEADERSHIP SERIES

PRINCIPLES

1

Prepare communications strategy in advance

2

Communicate clearly with different parties, tailoring message where necessary

3

Manage the aftermath in the medium to long term

References:

Guidance on effective communications in a cyber incident
Crisis Communication and Incident Response pt. 1
Crisis Communication and Incident Response pt. 2

LRQA

LEADERSHIP SERIES

INCIDENT MANAGEMENT

What we see works

Have and lean into your Incident Response Plan

- An incident response plan is one of the most critical components of the customer notification process, as it enables you to acknowledge they've fallen victim to an attack, but also take ownership and focus on the customer
- Following a data breach, the customer ultimately wants to know three things:
- If their data has been stolen
- The risk to the data at the time of the incident
- If they need to take additional action

Maintain open and consistent comms

- Time is of the essence – you must execute on customer communications as early as possible
- You need to be the go-to source for any information regarding a breach at all times
- Ideally, you should give affected customers a clear understanding of which data was lost and when the incident occurred
- Some of the top questions to ask your team when communicating a data breach include:
  - What happened and what do we know?
  - What is the scope of the incident?
  - How can we impact this, and how exactly can we help the customer?
- Do NOT move too fast and respond without having gathered the right information or assessment of impact, which can change the narrative!!!!

Be Transparent

- Where possible, provide accurate and timely information that accounts for customer questions and looks after their best interests while also adhering to internal and external legal advice to minimise liability
- If unable to share specific breach details (quite likely) – look at being transparent about the reason for not immediately releasing information publicly, i.e., if law enforcement is involved
- Never assume or share with your customers that it won't happen again…
- Assure the affected customer that the incident is being properly contained and managed
- Show that you are prioritising security and taking the necessary steps to mitigate future potential breaches as well

LRQA

LEADERSHIP SERIES

LRQA
Your Risk Management Advantage

THANK YOU

Any questions?

Jamie Roderick | jamie.roderick@lrqa.com

LEADERSHIP SERIES