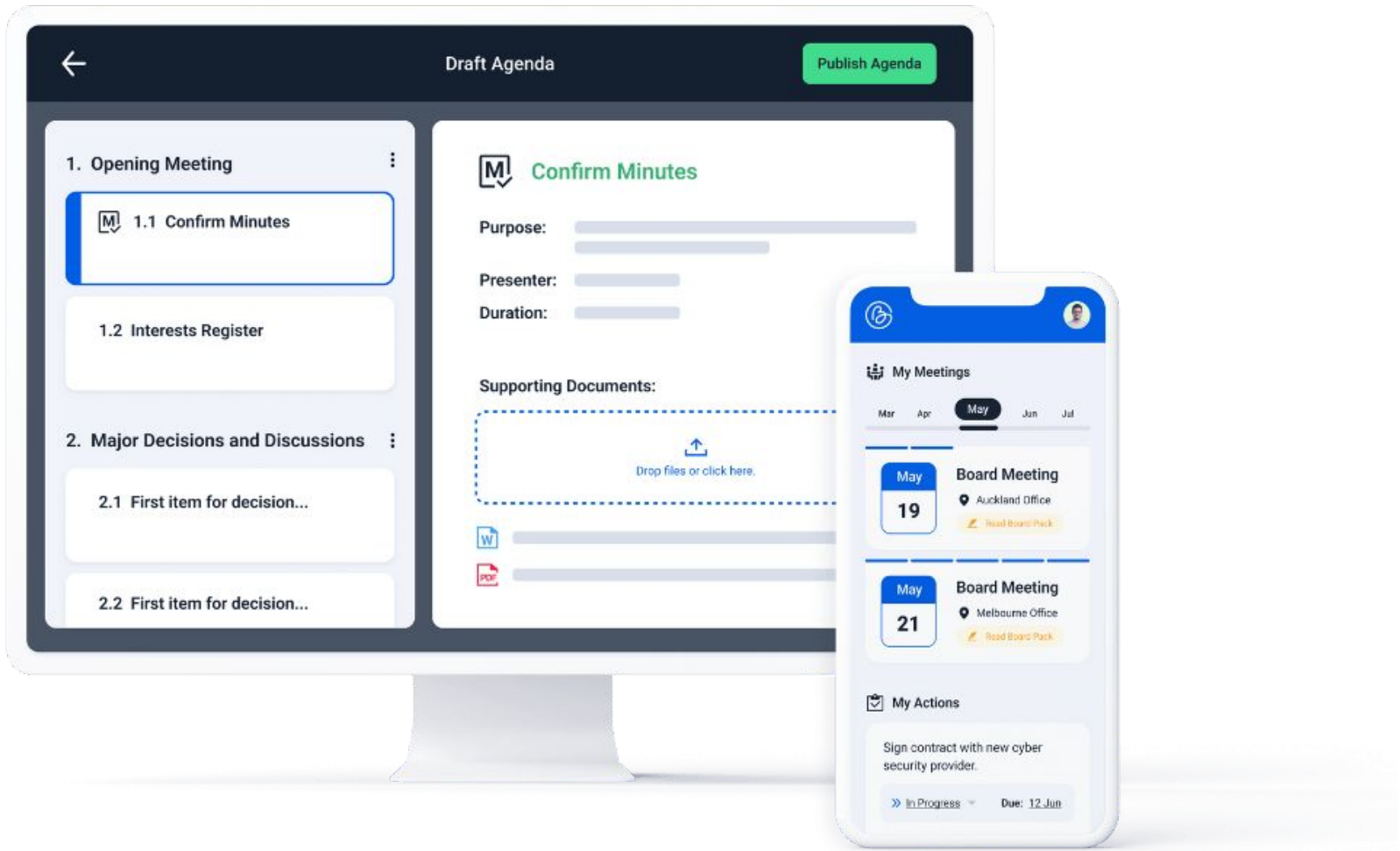
BoardPro™

Cyber Security

The board's role in overseeing cybersecurity and protecting against data breaches

With Steven McCrone


BoardPro™


Draft Agenda
Publish Agenda
1. Opening Meeting
1.1 Confirm Minutes
1.2 Interests Register
2. Major Decisions and Discussions
2.1 First item for decision...
2.2 First item for decision...
Confirm Minutes
Purpose:
Presenter:
Duration:
Supporting Documents:
Drop files or click here.
My Meetings
Mar
Apr
May
Jun
Jul
May
19
Board Meeting
Auckland Office
May
21
Board Meeting
Melbourne Office
My Actions
Sign contract with new cyber security provider.
In Progress
Due: 12 Jun

Making the fundamentals of governance free and easy to implement

Governance Made Easy

Governance Resource Center

Explore free governance resources for growing your organisation and adopting good governance practises. From meeting minutes templates to CEO reporting templates, our comprehensive guides and templates will cover your governance and business essentials.

Content type | Topic | Persona | Search

Slides, webinar video, transcript and slides will be sent to you. Sit back, relax and enjoy the conversation

Steven McCrone

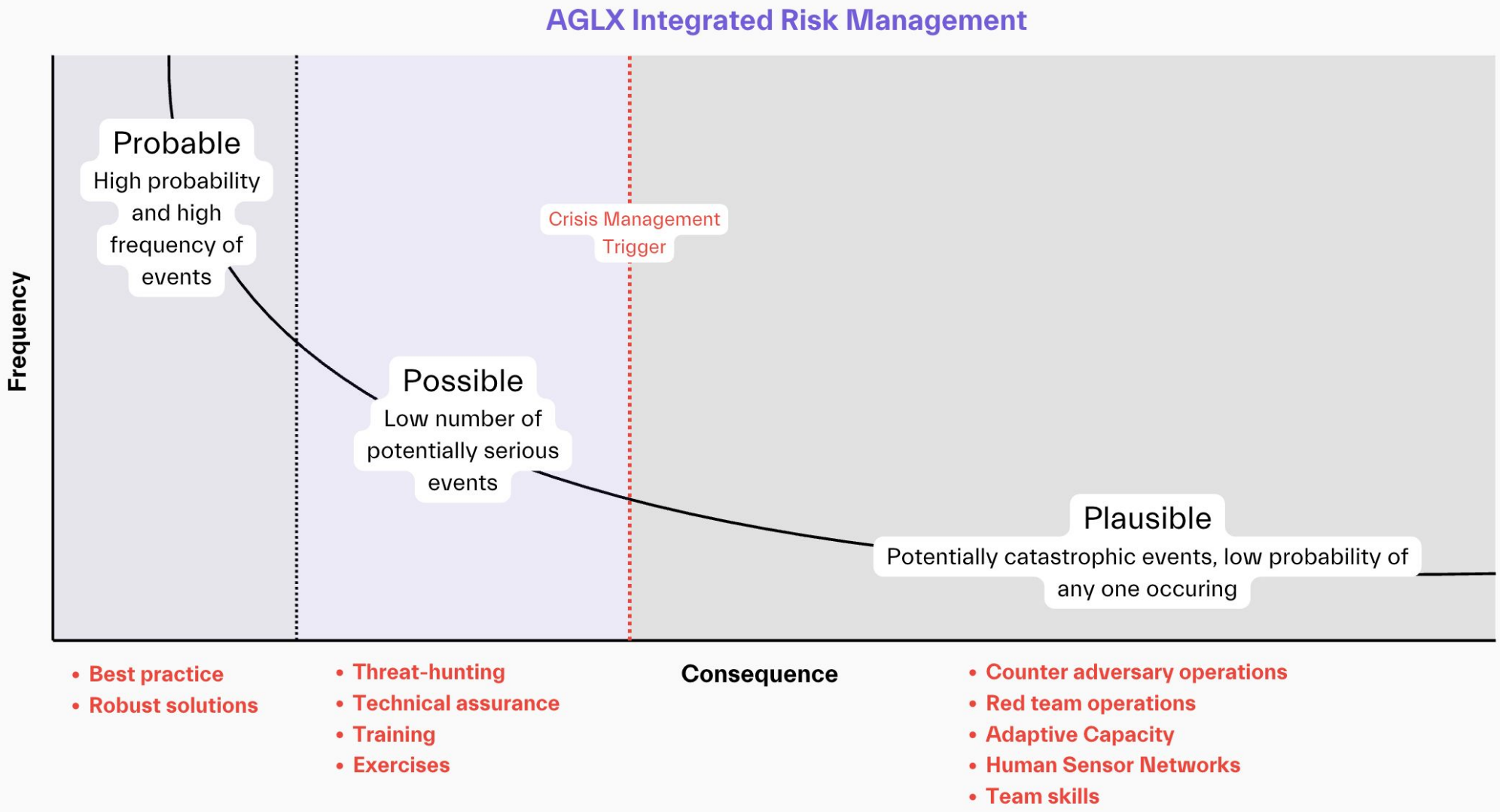
Managing Director
AGLX

Christopher Lloyd

Cyber Security Manager
Watercare Services

Amplification of Threat

AGLX



Amplification of Threat

AGLX

Adversarial


Nation-state actors


Targeted Cybercrime

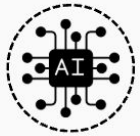

Opportunistic Cybercrime


Hacktivists


Insider threat


Influence operators

Systemic



Artificial intelligence


Geopolitical shifts


Antiquated technology


Big technology


Societal imbalance

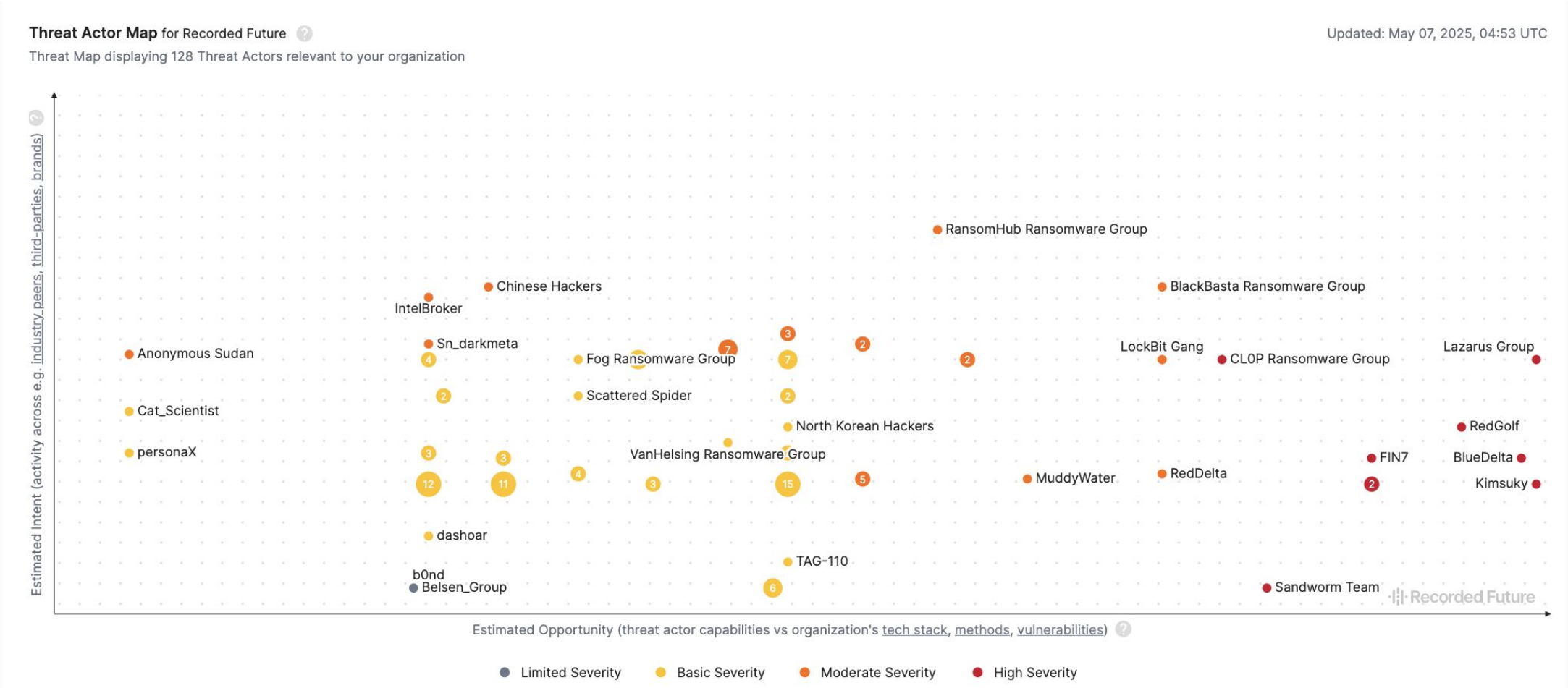

Quantum computing

Amplification of Threat

AGLX

418 Ransomware Incidents

- Qilin (Agenda) Ransomware Group (70)
- Akira Ransomware Group (48)
- Play Ransomware Group (47)
- Lynx Ransomware Group (32)
- Other (221)



The Changing Context

AGLX

Cybercrime has evolved into a highly profitable global enterprise. Like it or not, your organisation is directly involved in this industry. As participants in the cybercrime industry our best strategy is to:

- Increase the cost (time and energy) for cybercriminals to engage with us.
- Decrease the value they can expect from that engagement.
- Utilise the information we gain from interactions with cyber criminals.

We need to shift from a defensive mode to an active mode. Passive defenses are important but leave us vulnerable to emerging risk. We need to build resilience through action.

Resilience = Maturity + Adaptive Capacity

Police raid on a professional cyber criminal organisation.

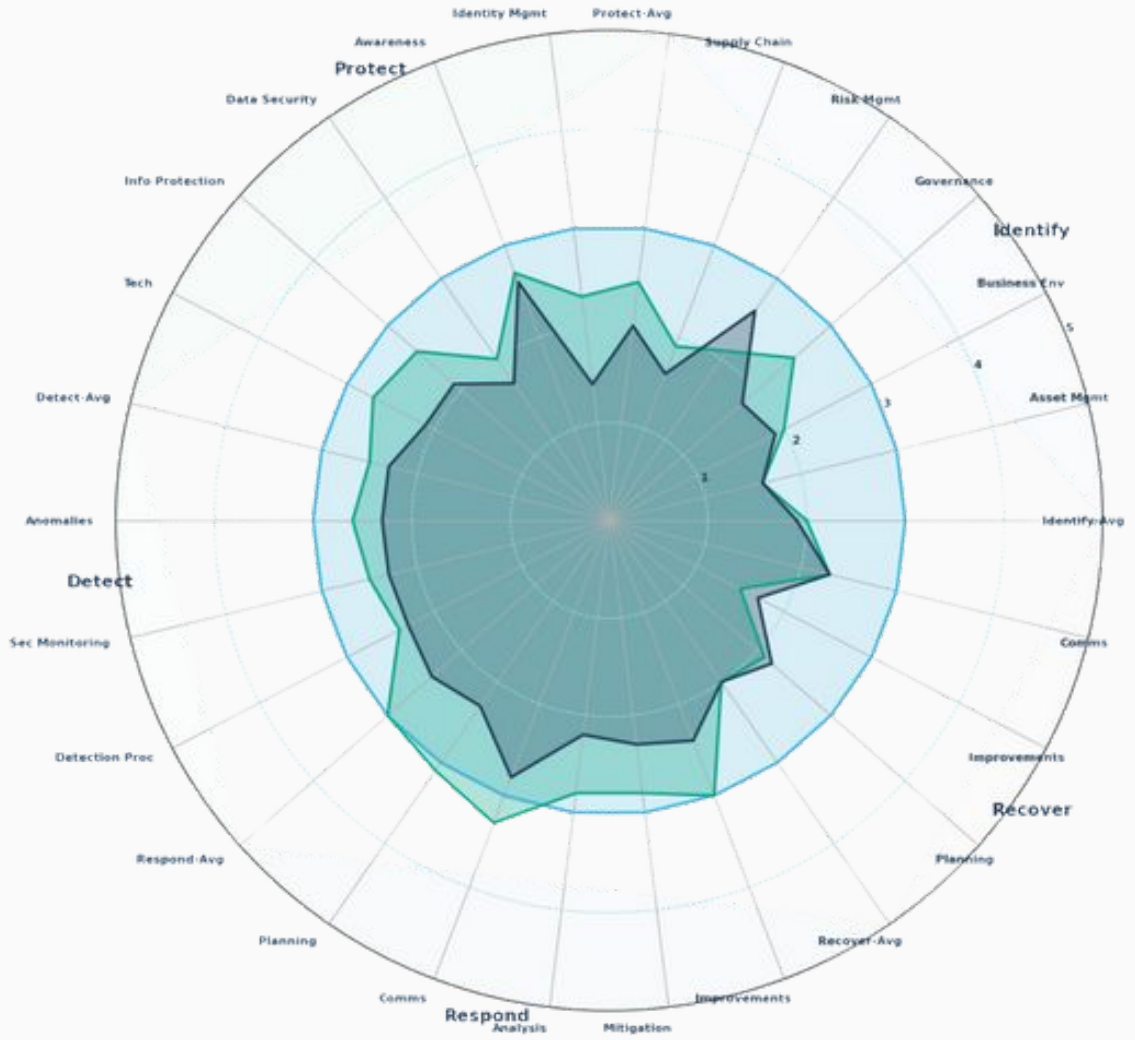
Maturity

AGLX

Represents the baseline level of preparedness and is ideal for addressing probable, predictable risks.

We advise clients to adopt standardised security controls, frameworks and processes. NIST Cybersecurity Framework, ISO 27000 standards etc.

We can establish benchmarks and expectations regarding our ability to govern, identify risks, protect critical systems, detect, respond and recover from cyber attack.



Adaptive Capacity

AGLX

The ability to achieve specific, desired outcomes by leveraging governance, skilled personnel, streamlined processes, and advanced technologies as foundational components.

Focus on creating the capability to respond to targeted, sophisticated, or catastrophic cyber incidents.

This can include active engagement such as deception, threat profiling, purple teaming etc.

Strengthen workforce capacity by developing essential knowledge, skills, and abilities (KSA's).

Intelligence-driven exercises that simulate real-world threats.

This practical experience will reinforce preparedness.

Threat readiness

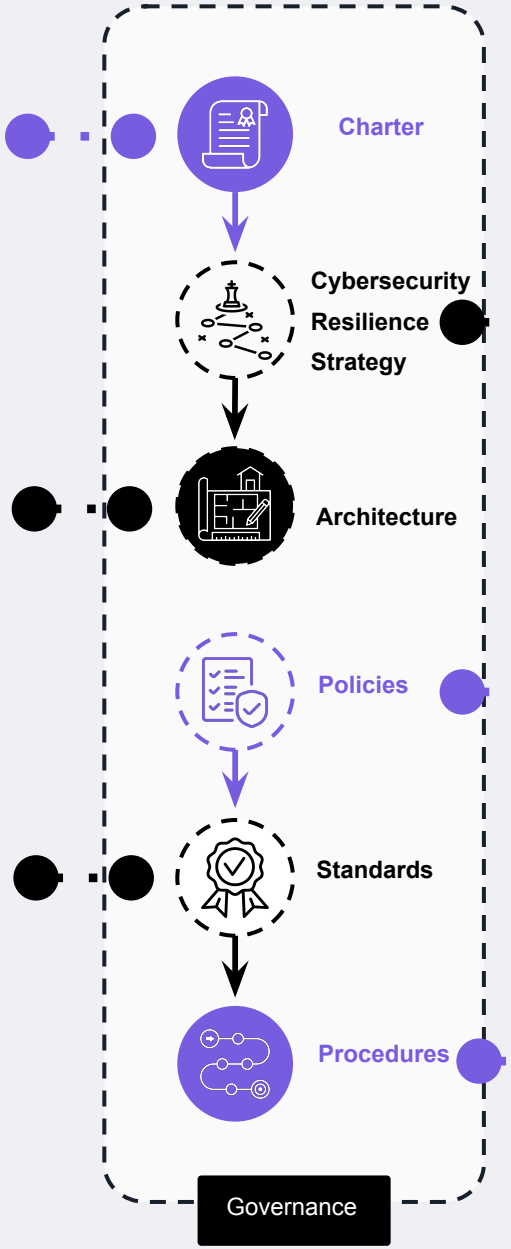
1. **Learn** KSA from experts, mentors and peers.
2. **Practice** using KSA as individuals & teams.
3. **Experience** using KSA wile leveraging experience from partners and experts against modern threats.
4. **Update** KSA over time as technologies and threats evolve, learn from experience and share our experiences with other organisations.
5. **Apply** and validate skills through certification as individuals and teams.

From Intent to Action

The cybersecurity charter provides the authoritative stakeholders **statement of intent** for cybersecurity, this document gives the authority to the cybersecurity program and capability. This document also **defines the authority** to act on certain risk scenarios

Enterprise Security Architecture (ESA) is a structured framework that **aligns** an organisation's **security practices, technologies, and processes** with its business objectives and risk management requirements.

Security standards define the parameters for implementation of **security practices, configurations, and controls.**



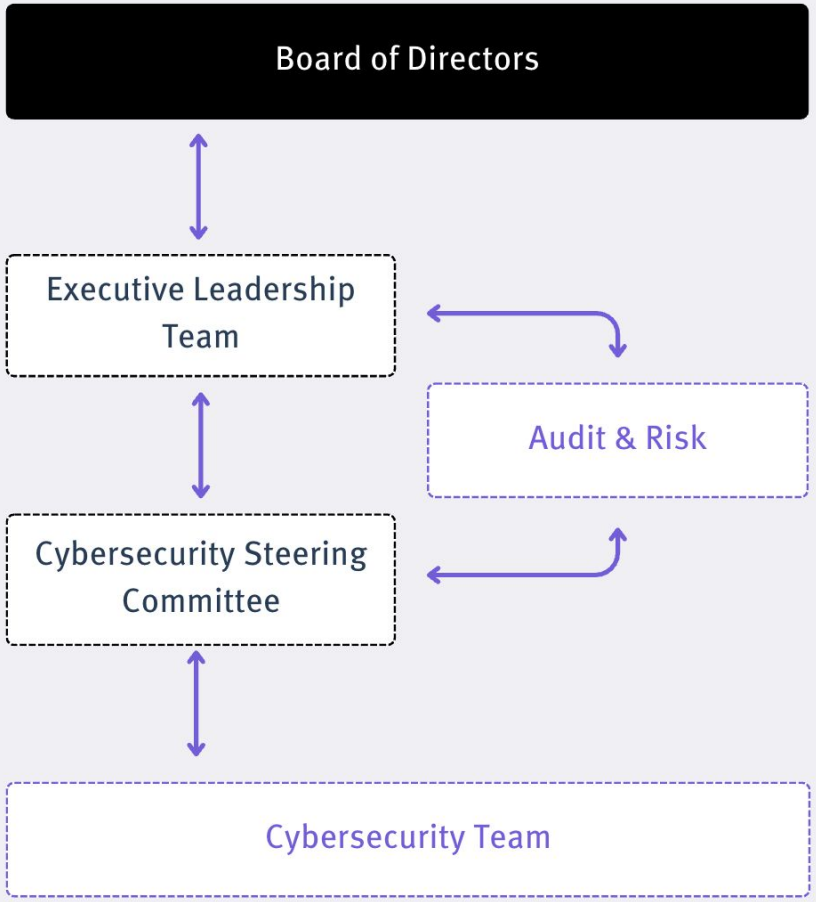
The '**Adaptive Cybersecurity Strategy**' outlines the **vision , intent and roadmap** to deliver the required capabilities and maturity to **execute the business mission.**

Policies are **high-level statements of intent** from executive leadership that outline the organisation's approach **to security across various domains**. They define roles and responsibilities, setting clear expectations for who is accountable for specific security actions and decisions

Procedures are **detailed,** step-by-step **instructions** created by business units to guide the execution of tasks and processes in alignment with established security standards.

Role of the Board

AGLX



Board (with Audit and Risk Committee)

- Set expectations for the cyber strategy
- Compliance with regulatory requirements
- Alignment with organizational risk policy
- Resource allocation
- Share and learn from other organisations

Larger organisations may need a steering committee to help with technical or specialist advice.

The Executive and Cyber team

- Building capability and maturity
- Build adaptive capacity
- Minimise attack surface
- Increase complexity for potential attack
- Robust incident response
- Workforce culture and competency

Measures of Success

AGLX

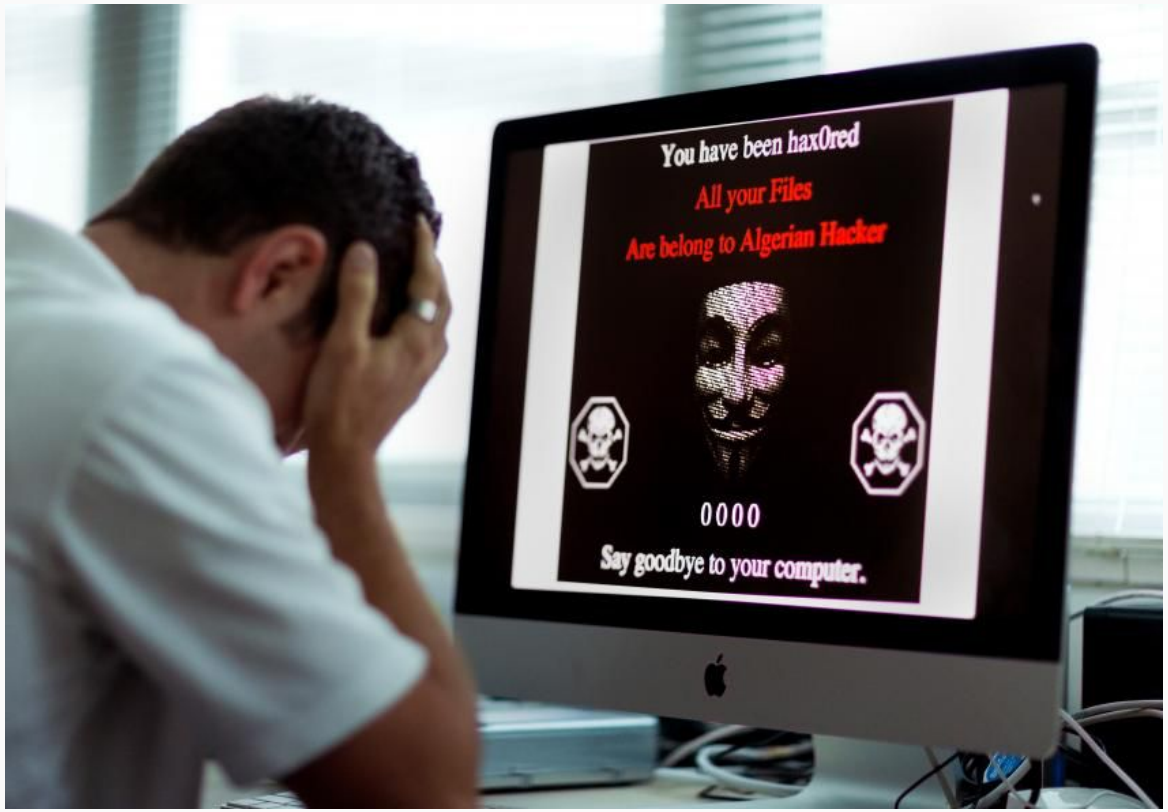
Categorical measures are useful but can lead to defensive measures that become vulnerable over time. Measures should include the things that provide evidence of increasing maturity and capability. For Example:

Maturity

- Assessment against the NIST and IEC frameworks
- Benchmarking against similar organisation's
- Capacity for threat identification – real time sensemaking, active intelligence
- Identified threats and risks have a mitigation plan
- Regular pen testing

Adaptive Capacity

- Capacity to act quickly – waiting months for a business case to be approved is a risk
- Staff training / Exercises
- Qualitative measures on our capacity to respond
- Continuous Threat Exposure Management
- Red / Purple teaming



Steven McCrone

www.linkedin.com/in/**stevemccrone**

Christopher Lloyd

www.linkedin.com/in//**christopherlloydnz**

BoardPro™

Thank you