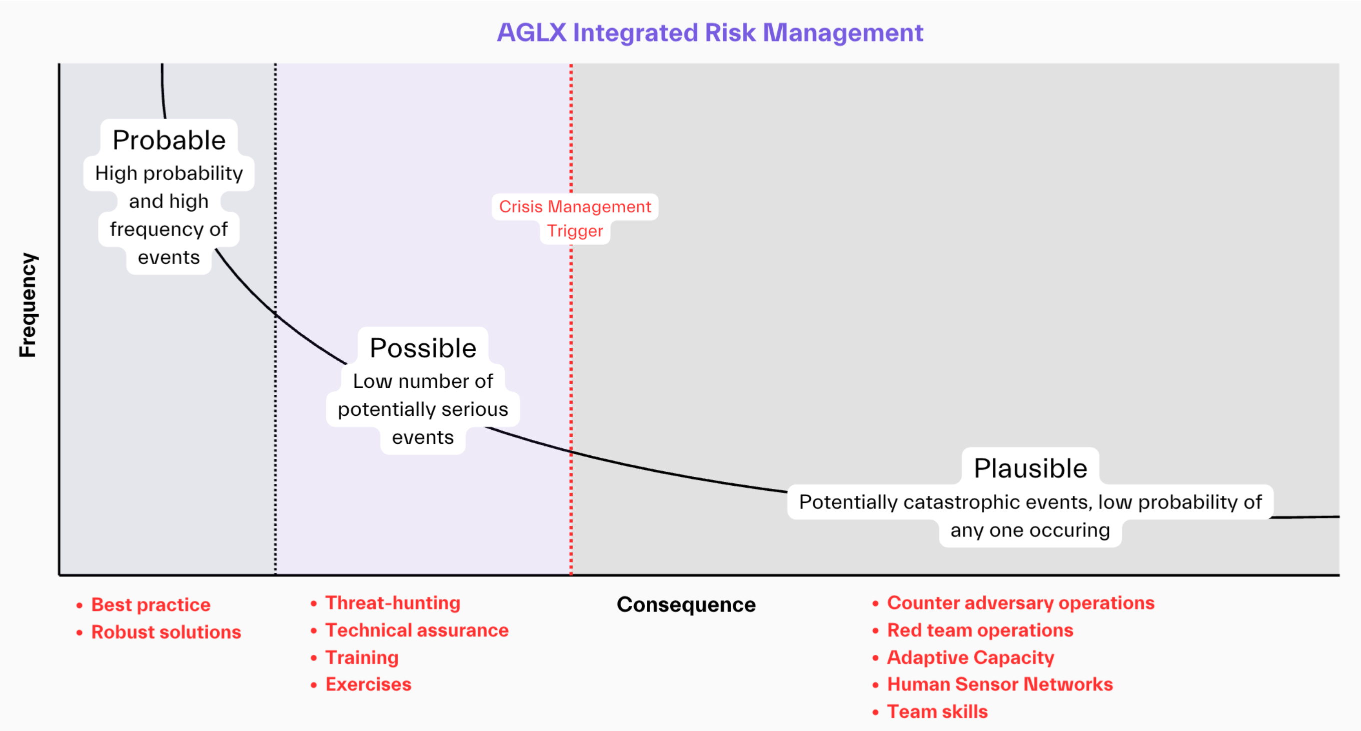
The Boards Role in Overseeing Cyber Security

THE EVOLVING CYBER THREAT LANDSCAPE


AGLX Integrated Risk Management
Frequency
Consequence
Probable
High probability and high frequency of events
Crisis Management Trigger
Possible
Low number of potentially serious events
Plausible
Potentially catastrophic events, low probability of any one occuring
• Best practice
• Robust solutions
• Threat-hunting
• Technical assurance
• Training
• Exercises
• Counter adversary operations
• Red team operations
• Adaptive Capacity
• Human Sensor Networks
• Team skills

We face an increased frequency of probable, possible, and plausible cyber events, driven by systemic risks and a dynamic adversary landscape. AI is accelerating this change.

Threat actors are highly motivated and sophisticated. They are **opportunistic**, often targeting organisations based on their vulnerability. Organisations operating on **dated infrastructure** are increasingly vulnerable.

Cyber crime is a **global business**; you cannot opt out. Attackers are organised professionals, operating like businesses with structures resembling marketing, HR, and even finance functions for money laundering. The **pressure for attackers to innovate is higher** than for defenders. They rapidly leverage new technologies like AI without the governance hurdles and business inertia legitimate organisations face.

You cannot create the conditions where you are immune from attack.

Resilience means creating the conditions where cyber criminals must commit more resources attacking you than they will gain from that attack – **make your organisation a bad investment**.

GOVERNANCE AND STRATEGIC ALIGNMENT

Good governance is an **enabler**, providing the necessary framework and authority for the organisation to act decisively.

The **board's role is primarily strategic**: ensuring the organisational strategy supports the desired level of cyber maturity and capability. It is the executive and security team's role to implement this.

Your cyber security strategy must be **explicitly aligned to the organisation's mission**; The purpose is to protect that mission. This protection and the resources committed to it needs to be tiered:

- mission critical,
- business critical,
- business supporting.

Ensure that **appropriate authority to act is delegated** to key people. In a fast-moving cyber crisis, **decisions need to be made in minutes**, not hours or days waiting for higher-level approval. There must be **trust** in your senior leadership.

The Boards Role in Overseeing Cyber Security

STRATEGIC IMPERATIVE FOR BOARDS

Focus on Resilience and Adaptive Capacity

Business Continuity – Identify your mission critical systems and make sure those are protected. A critical measure is the **minimum time required to reconstruct mission-critical systems** after an incident.

Do it now. Organisations often only undergo significant digital transformation after a major cyber incident. A proactive strategy is to **assume you've been "absolutely owned" and identify necessary transformations now** to build resilience.

True resilience requires **adaptive capacity**, which must be **built into operations from the outset**, not added later. This involves **exercising and practising responses,** as plans alone are insufficient in a crisis. Techniques like **Chaos Engineering and Red Teaming** can build resilience by design.

Prioritise People, Process, and Competence: Effective cyber security is **not solely about acquiring the best security tools.** While tools are needed, **robust processes, competent people, and proactive strategies** are more critical, especially against emerging threats.

Compliance frameworks are useful but cannot be simply dragged and dropped; they must be tested in your specific context as attackers also know these frameworks. Adopt a compliance framework that suits the context of your organisation.

Build competence and processes first, understanding how to do things, then leverage technology to create efficiency and scale. Implementing expensive technology without underlying process and governance is likely to fail.

Adopt Continuous Awareness and Realistic Testing: Relying on **lagging indicators** (e.g. past incident reports) or point-in-time assessments (like traditional penetration tests) is **ineffective for driving future security decisions**. These snapshots are quickly outdated.

Invest pragmatically in **continuous awareness models. Continuous red teaming**, where a dedicated team constantly simulates attacks against your defences, provides invaluable, real-time insights and builds adaptive capacity under pressure.

Organisations often play "too nicely" by the rules; attackers do not. Continuous testing with an attacker mindset is key.

Develop a Robust Communications Strategy: Well-practised strategic communications are vital during an incident. Immature or inconsistent messaging damages reputation and undermines response efforts. Decide in advance on your approach to transparency. What will you make public? What will you keep private?

Communications can be part of a broader **deception strategy** during an incident, potentially influencing attacker behaviour or negotiations. Managing reputation is a key concern for boards.

Adaptive Cyber Security

- Understand the dynamic threat landscape, shifting focus from prevention to **building an adaptive, resilient organisation**.
- Ensuring **strong governance aligned to the mission with delegated authority,** and having a **well-defined communications plan**.
- Prioritising **people, process, and competence over technology**.
- Adopting **continuous and realistic testing**.

By focusing on these strategic areas, you can significantly enhance your organisation's ability to navigate the complex cyber threat landscape.

Contact Us:

Steven McCrone
Managing Director
Email: Stevem@aglx.com

Website:
www.aglx.com