

Governing Through a Cyber Crisis

Strategies for Execs & Boards

Gaurav Vikash

Head of Security and Risk – Axon (APAC)

ROLE



GUIDE

People, Process, Tech



FORESEE

Short & Long-Term Impacts



GOVERN

Involvement, Oversight



GUIDE



PREPARE FOR THE EVENTUAL CRISIS

VALIDATE

Risk and Threat-Based Incident Tests

Timely Availability of Resources

Well-Defined Roles & Responsibilities

Internal and External Comms

RED FLAGS

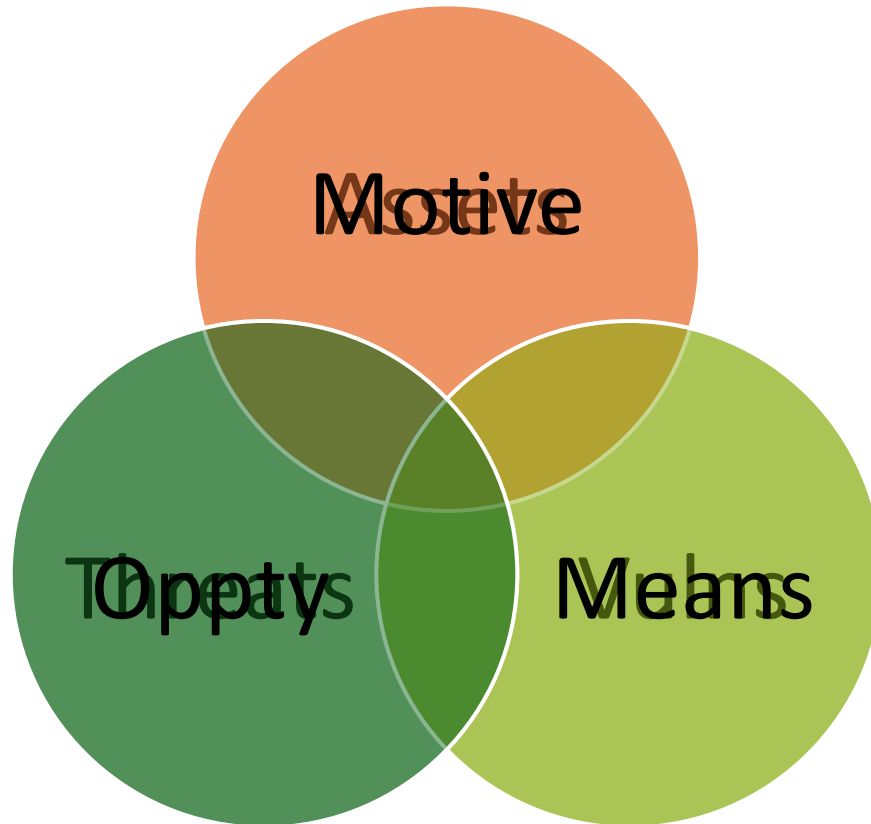
None or Irrelevant Assessments

Lack of Funding, Skills, Industry Support

Assumptions, Lack of Documentation

Undefined Role, Cultural Issues

RISK & THREAT-BASED INCIDENT TESTS



COMMON MO

Ransomware & Data Breach

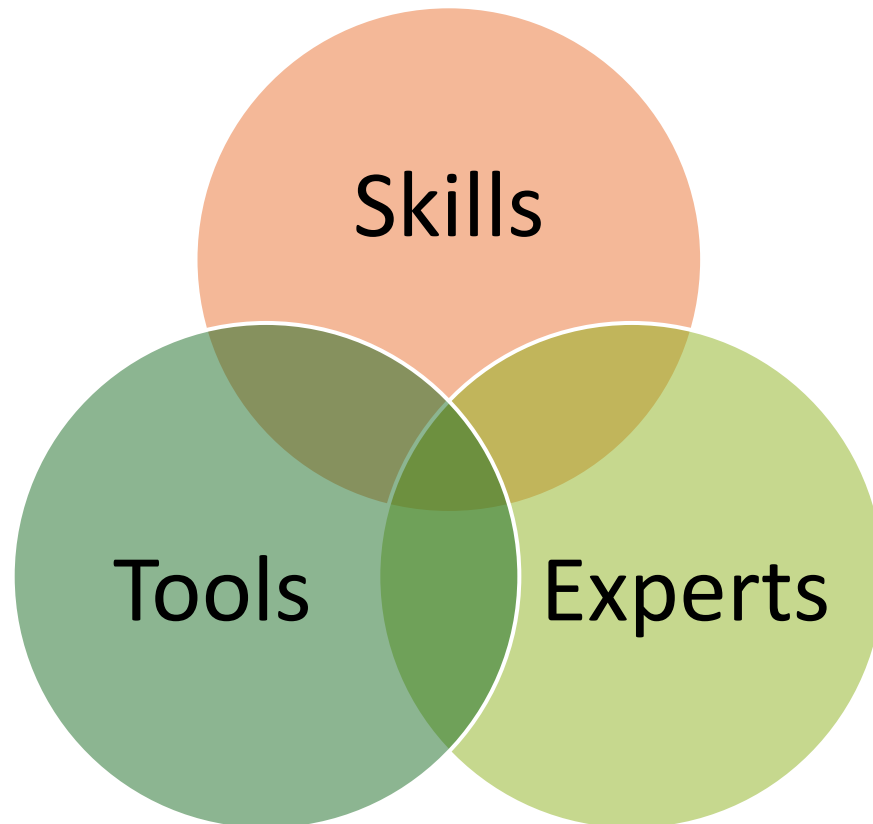
Insider Threat

Supply Chain Weaknesses

Critical System/Software Failure

Payment Redirect

RESOURCES AND RACI



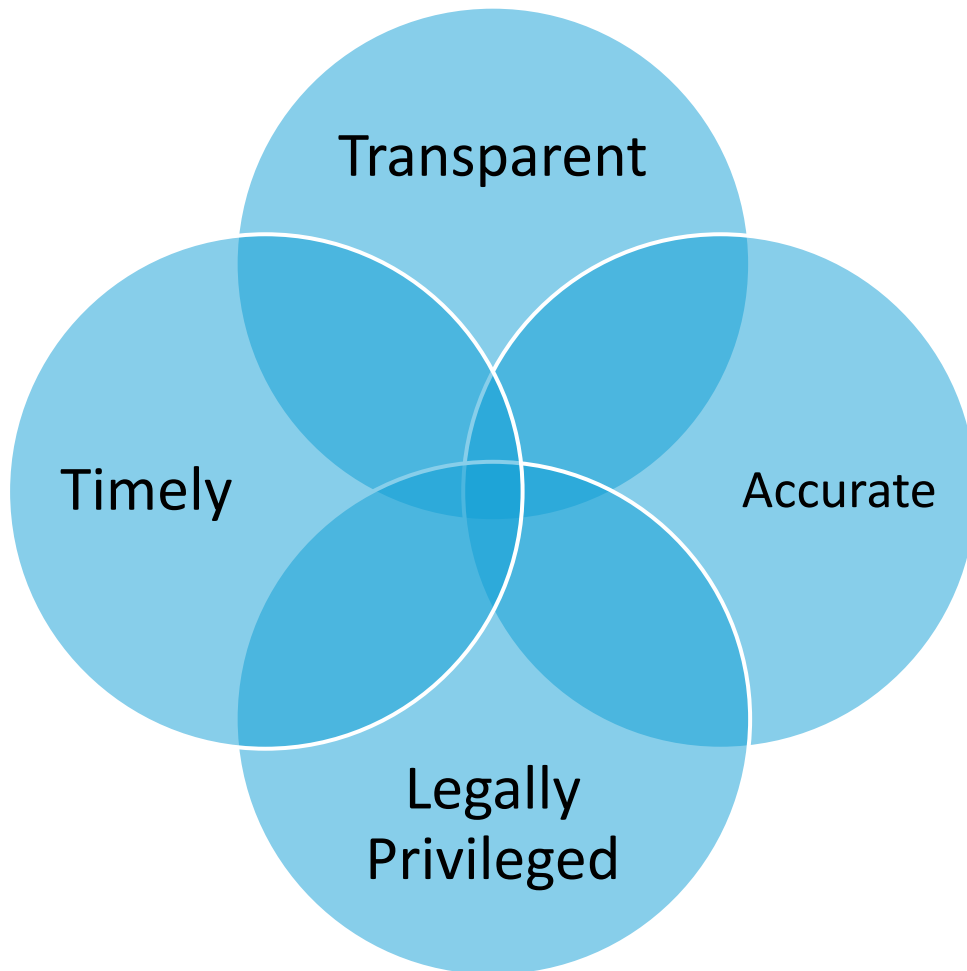
KEY CONSIDERATIONS

Internal and External Expertise

Prevention and Forensic Tools

Whole-of-Organisation RACI

COMMS



KEY

Contr

Regul

Accur

Prom

Owne

“

Clear, transparent communication is the lifeblood of navigating a cyber incident. It fosters trust, calms anxieties and helps rebuild reputation.”

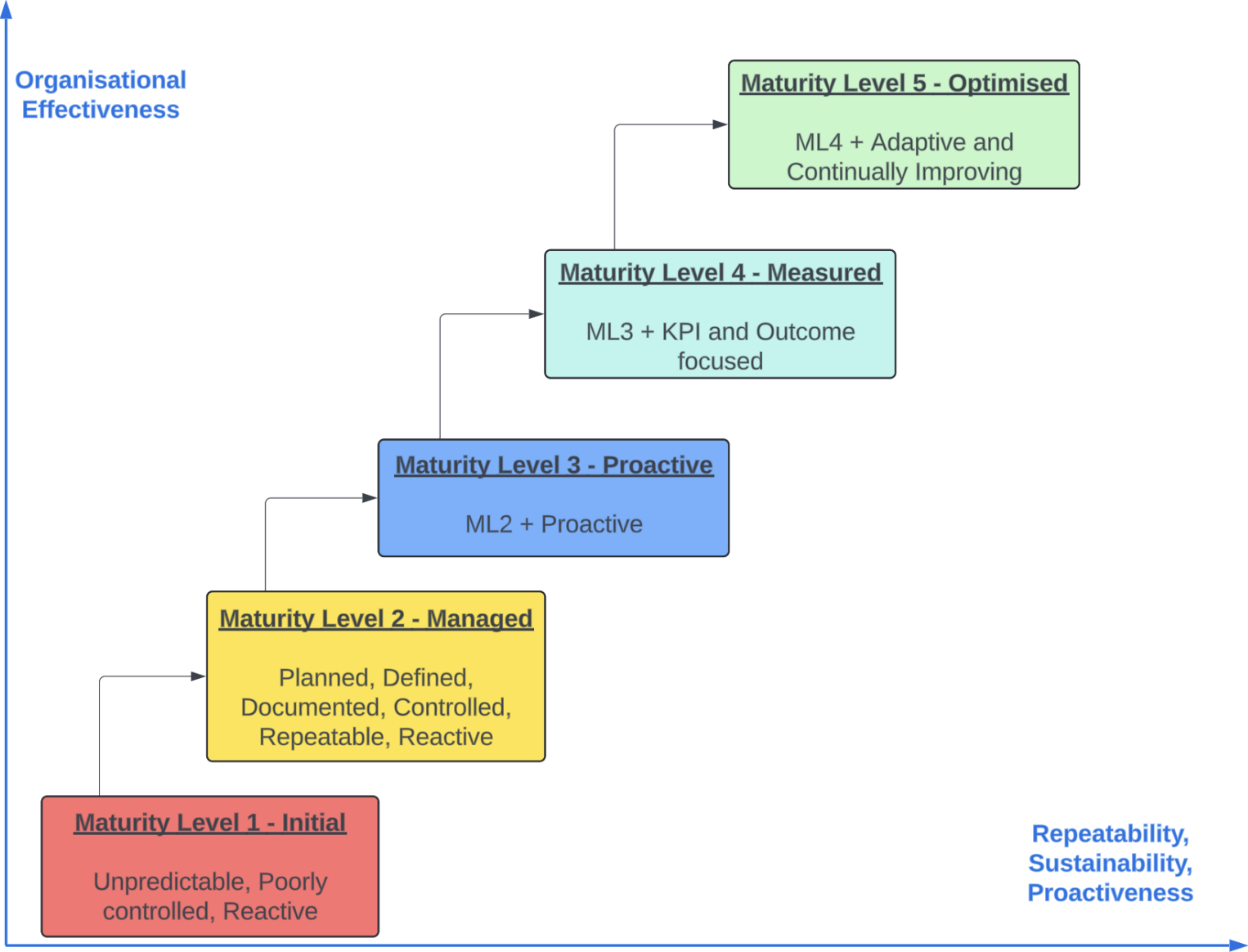
— Senior director
ASX listed-company

ns

is

on

Cyber Resilience Maturity Model



KEY CONSIDERATIONS

Reactive vs Proactive Capability

Whole-of Org Response

Regulation, Contract, Perception

Skills, Scale, Forensics, Speed

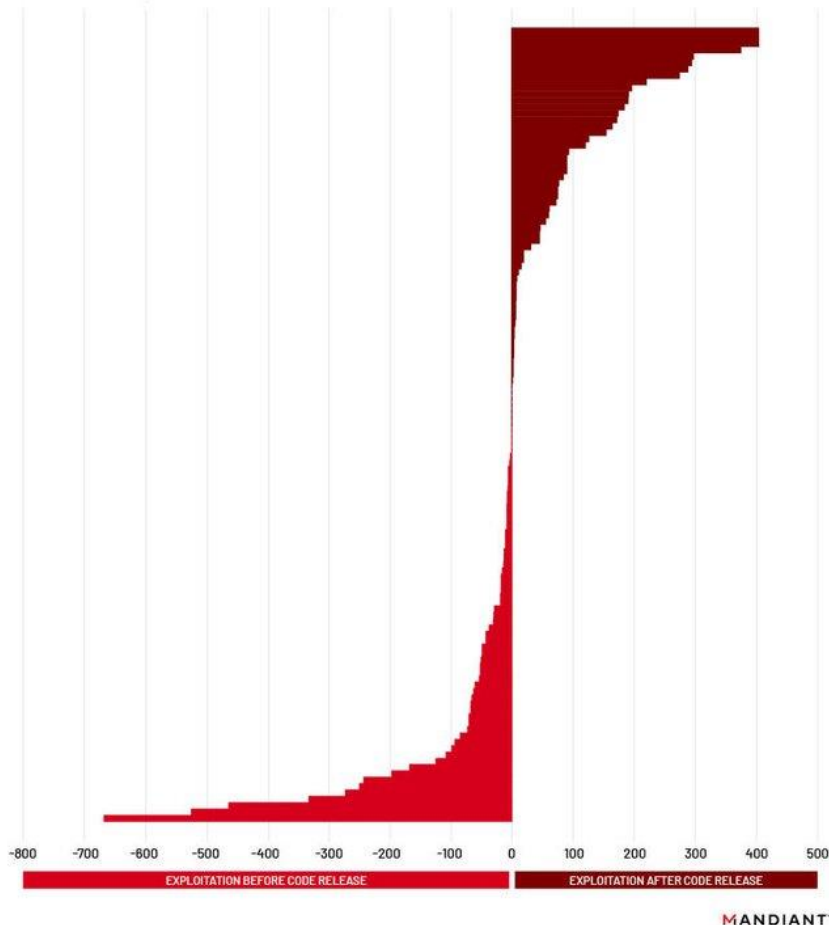
Accountability, Comms, People

FORESEE



SHORT & LONG-TERM IMPACTS

Days Between Exploit/PoC Code
and Exploitation



KEY CONSIDERATIONS

Real-life Impact to Affected People

Wellbeing of the Staff

Cost, Speed, and Scale of Recovery

Customers, Government, Regulators,
Other Key Stakeholders' Expectations

Reputation, Litigation, Repeat, Solvency

GOVERN



GOVERN - DURING THE CRISIS



Understanding of the Impact and Impacted Stakeholders



Agile and Timely Support and Oversight of Leadership Decisions



Consistent, Timely, and Transparent Internal and External Comms



Wellbeing of All Involved Stakeholders, Including Staff



Expert Technical and Forensic Investigation

“

When a cyber crisis occurs you know you have to act fast but until it happens to your organisation you don't realise how fast.”

— Senior Chair, ASX-listed company and NFP

“

Be really clear about who your critical stakeholders are, how you communicate with them and who communicates with them.”

— Senior Chair, ASX-listed company

GOVERN - AFTER THE CRISIS



Rebuild Reputation, Manage Perceptions



Support Customers, Regulators, Staff, Others



Reassess and Uplift Readiness for Future



Transparent, Clear and Empathetic Comms



Uplift Self Awareness

“

When you're a chair, you've just got to drop everything and be there.”

— Senior Chair, ASX-listed company

CONCLUSION

GUIDE

- Leaders need to be confident their organisation is cyber ready. The benchmark is thorough and comprehensive planning for significant cyber incidents and business continuity.

FORESEE

- Leaders need to contemplate, from the outset, the long tail of potential post-incident risks, including people, financial, regulatory, operational, and reputational.

GOVERN

- Leaders should be actively involved in a cyber crisis.



Thank You!

Gaurav Vikash

