CYBER SECURITY CHECKLIST

QUESTIONS EXECUTIVES AND BOARD DIRECTORS SHOULD ASK:

SECURITY APPLIES TO THE ENTIRE ORGANISATION NOT JUST TECHNOLOGY.

"Amateurs hack systems, professionals hack people."
- Bruce Schneier

GOVERNANCE

1. What is our cyber security risk exposure?
2. Do we have a cyber security strategy?
3. Is this strategy refreshed annually, and aligned with corporate strategy and business operations?
4. Do we have a cyber security business engagement model?
5. What is our state of readiness in case of an attack or an incident?
6. Do we have an incident response management policy, plan, and capability?
7. Is there a Governance Risk & Compliance system in place including an executive dashboard and board reporting process?

CULTURE

1. Is every member of staff, employee, and supplier aware of cyber security risks?
2. Do we have cyber security awareness training being delivered regularly?
3. What is our level of cyber security maturity?

RISK EXPOSURE

1. Do we have an Enterprise Risk Management system covering cyber?

CYBER SECURITY CHECKLIST

THIS CHECKLIST BASED ON OUR EXPERIENCE AND A REVIEW OF MORE THAN 100 BOOKS, WHITE PAPERS, REPORTS, AND WEBSITES

2. Do we have an up-to-date cyber security risk management policy?
3. Do we have a board approved cyber security risk appetite and risk tolerance statement?
4. How many outstanding cyber security risks are there? Is there an aging report for outstanding cyber risks?

REGULATORY COMPLIANCE

1. What are the key regulatory compliance requirements that apply to our industry and our business?
2. When was the last cyber compliance audit done and what were the results?
3. Are there any outstanding or unresolved cyber security compliance issues?
4. Has the organisation implemented Australian Signals Directorate Essential 8 Controls?
5. What cyber security standards has the organization implemented?

TECHNOLOGY

1. Is our Security Operating Centre performing at optimum levels?
2. Do we have an IT asset register that clearly identifies all systems?
3. Is there a data governance policy in place including data classification and data loss prevention procedures and tools?