“Addressing Cybersecurity challenges through IT Security Governance”

Ravi Jayasundera

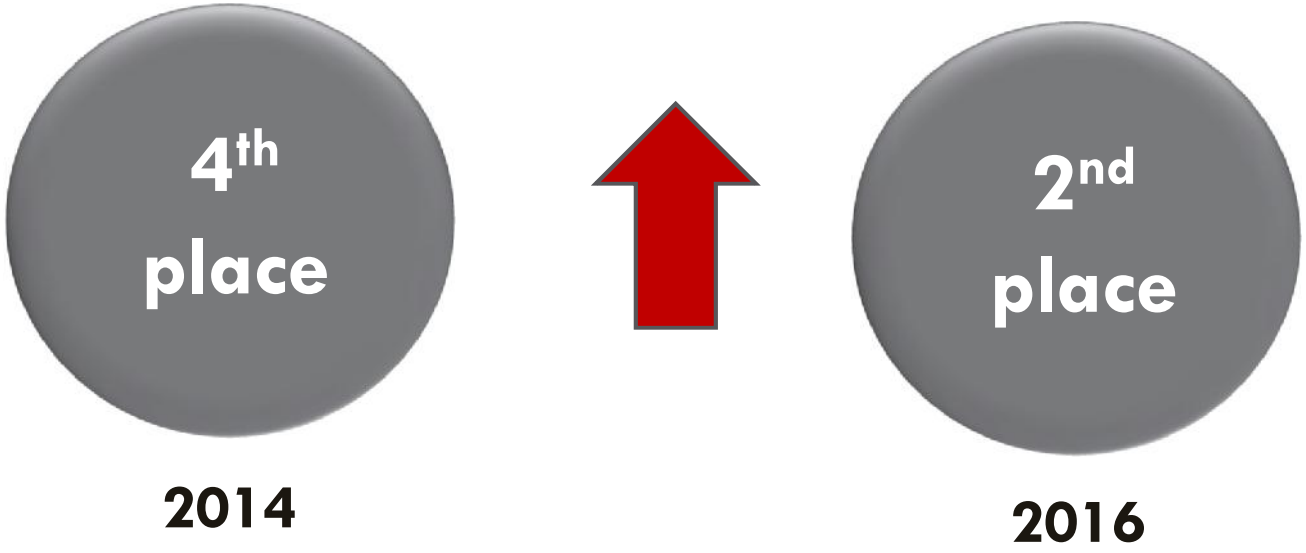
CEO

21st Sept 2016

Agenda

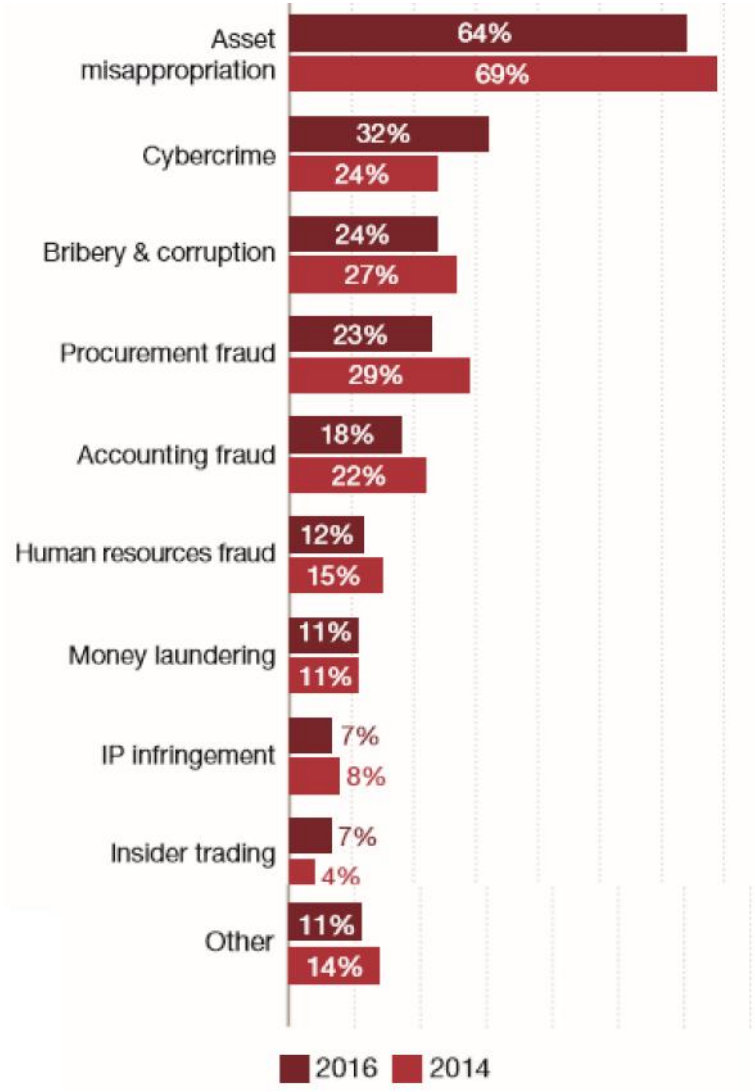
- Cyber crime moves up the order
- IT Security Governance
- Cybersecurity challenges
- Need for IT Security Governance
- Supporting frameworks
- Underlying principles
- Case study

Cyber crime moves up the order



PWC – Global Economic Crime Survey, 2016

PWC – Global Economic Crime Survey



Breach at law firm ‘Mossack Fonseca’

Bangladesh Central Bank

Source: Thompson Reuters, 2016

SYSPROVE CONSULTING

Need for IT Security Governance

- Demonstrate a cohesive approach towards information security
- Move from an operational IT to a business risk issue
- Accountability for security & risks
- Custodian vs Ownership of information

SYSPROVE CONSULTING

IT Security Governance

"Establish and uphold a culture of IT security to provide assurance that the **business objectives** and stakeholder requirements for the protection of information are continually met."

Australian Government Trusted Information Sharing Network (TISN)

"Processes that ensure reasonable and appropriate actions are taken to protect the organisation's information resources, in the most effective and efficient manner, in pursuit of its **business goals**"

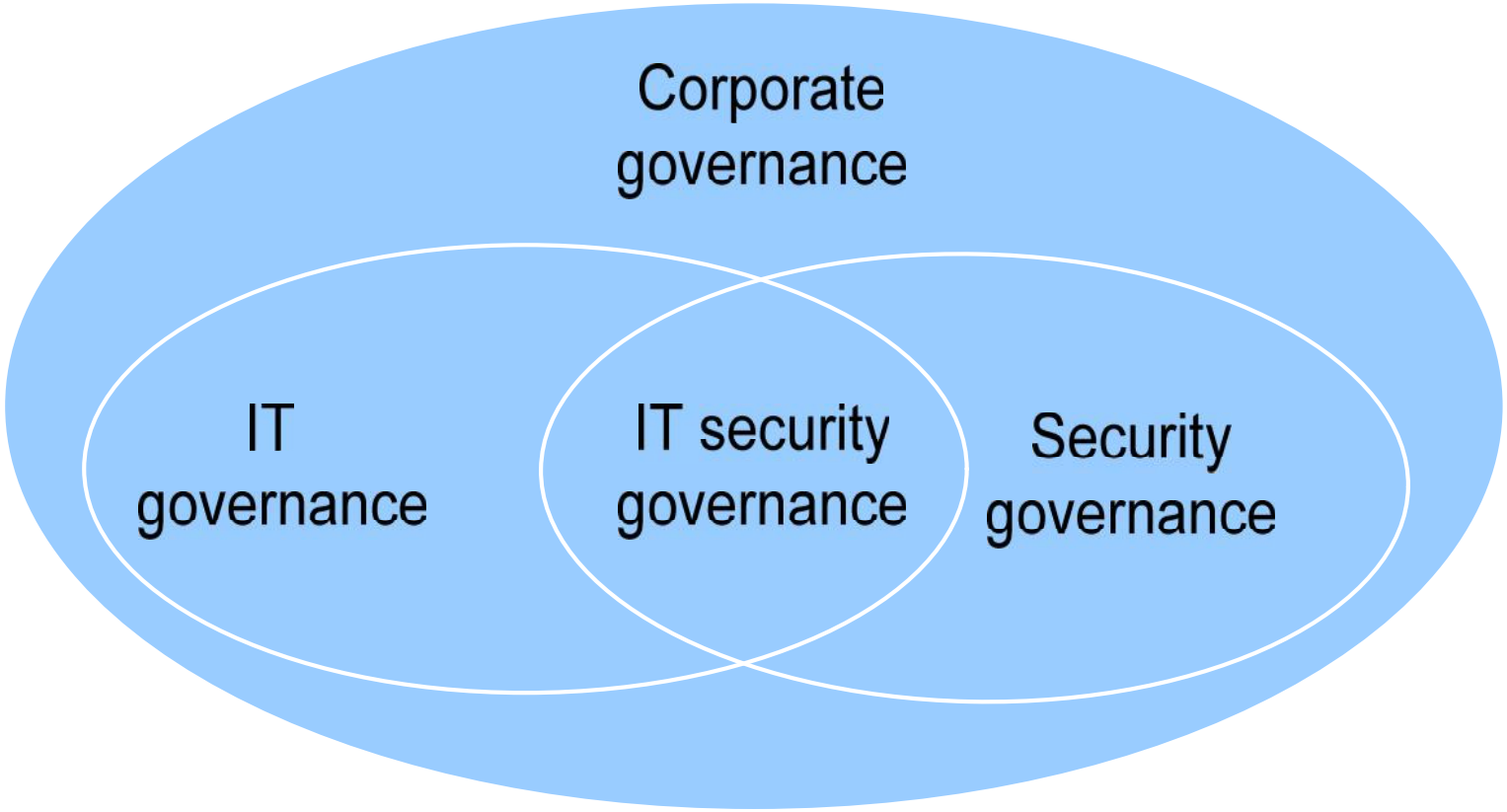
Gartner®

"System by which an organisation's information security activities are directed and controlled"

ISO /IEC 27014 : 2013

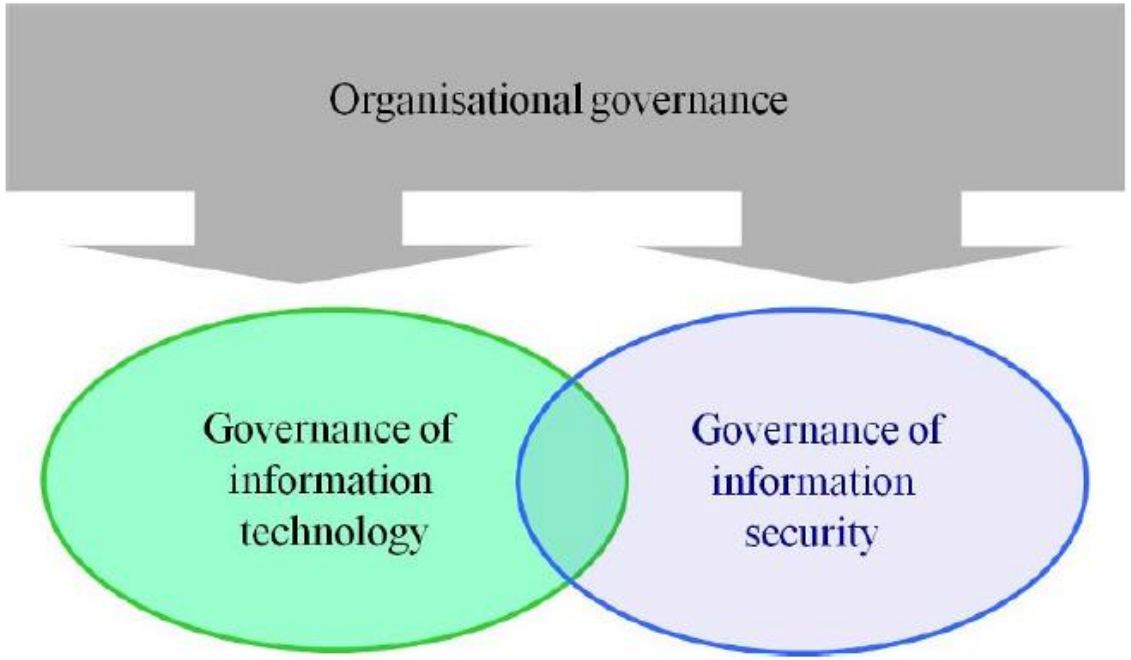
SYSPROVE CONSULTING

Corporate, Security & IT Governance



Source: Australian Government Trusted Information Sharing Network (TISN)

Organisational, IT and Information Security Governance



Source: ISO/IEC 27014 : 2013

Frameworks supporting IT Security Governance

ISO/IEC 27001:2013

ISO/IEC 27014 : 2013

COBIT 5 AN ISACA® FRAMEWORK

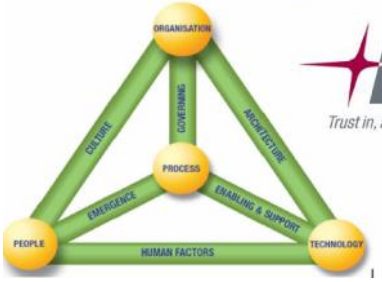
ITIL®

PCI Security Standards Council

NIST National Institute of Standards and Technology U.S. Department of Commerce

SABSA®

The Business Model for Information Security



ISACA® Trust in, and value from, information systems

SYSPROVE CONSULTING

Underlying principles

Based on : ISO/IEC 27014:2013

- Establish organisation-wide information security
- Adopt a risk-based approach
- Set the direction of investment decisions
- Ensure conformance with internal & external requirements
- Foster Security Positive environment
- Review performance
- Continual Improvement

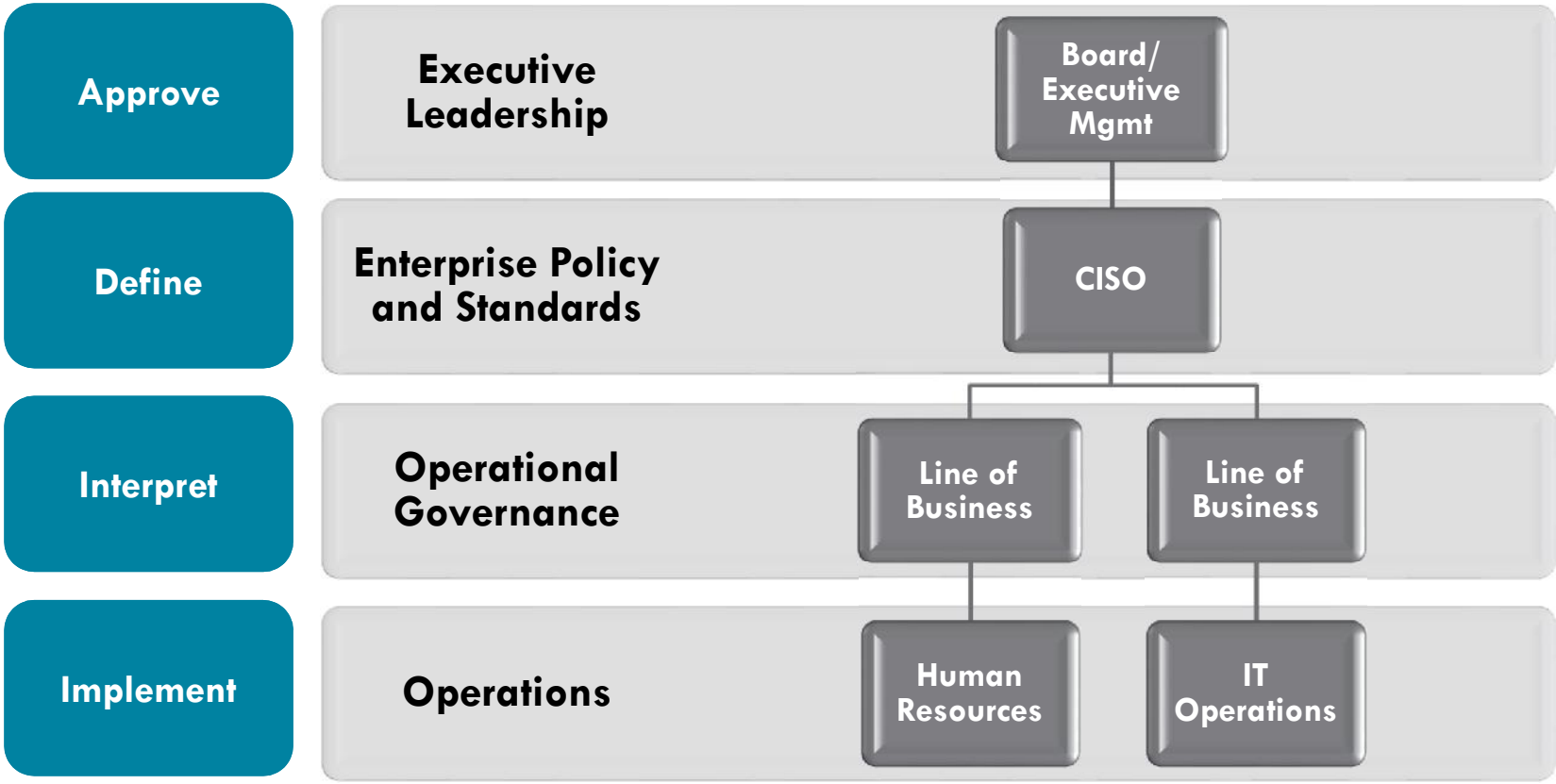
SYSPROVE CONSULTING

Approach

Accountability	• Board / Senior management accountability • Suitable structures • Info security charter • Policy framework
Risk Management	• Understand the risk appetite • Regulatory requirements • Link to corporate risk management - ERM / BCM • Manage conflicting requirements
Budgets & Resources	• Define budgets and allocation based on strategy • Alignment of projects with IT security
Supporting processes & architecture	• Manage between conflicting interests and harmonisation • Human factor • Information security priorities should be communicated • Ability to Predict, Prevent, Detect & Respond • IT Security Incident Management / Internal CERT
Measurement & Reporting	• Providing the assurances and adjustments required • Ongoing monitoring reporting back to Board

SYSPROVE CONSULTING

Supporting organisational structure



Case study

Leading MTO, Operating in the ME region, regulated by multiple regulators

Challenges

- Increasing Correspondent banks and regulators requirements for assurances on info security
- 'Knee-jerk' reaction to IT Security strategy / spending
- Limited involvement of Board / Executive management
- 'Passing the buck' to IT
- Limited policies, procedures and implementation

IT Security Governance

- Established Info Security Charter
- Cross-functional Working Group of Subsidiaries and key Departments
- IT security incident process maturity
- Implement supporting P&Ps
- Continuous improvement cycle

Result

- Senior Management appreciates the IT Security spending
- Commendation from Central Bank
- Increased the number of correspondent banks
- All initiatives have a key consideration for info security

SYSPROVE CONSULTING

In conclusion

- Requirement to further enhance the maturity of IT Security Governance
- Don’t re-invent the wheel
- Communicate
- Adapt to suit the organisation
- Continuously improve

SYSPROVE CONSULTING

Thank you

www.sysprove.com ravi@sysprove.com

Follow us on:

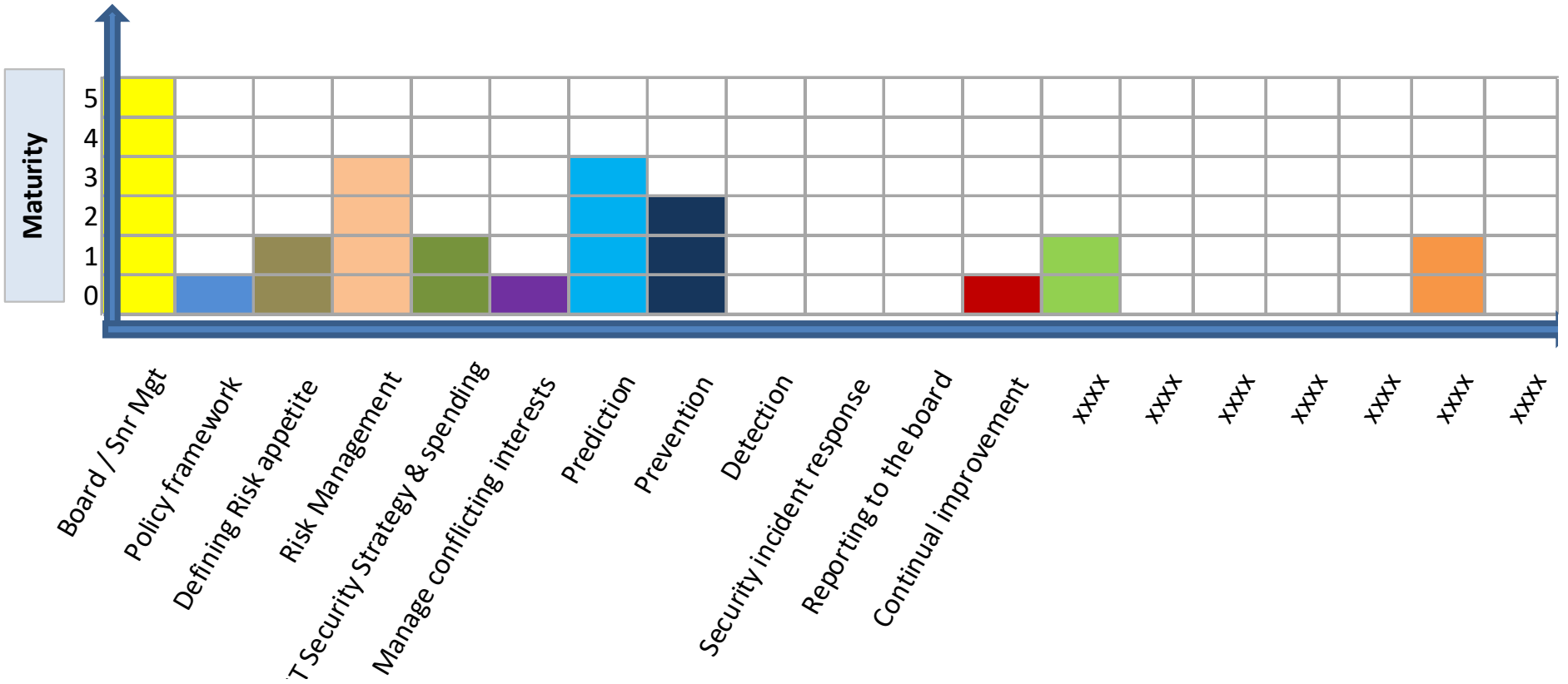
 @Sysprove

 @Sysprove

 @Sysprove

SYSPROVE CONSULTING

Developing the maturity



Identify the 'As-Is' and 'To-Be' and the Gaps

SYSPROVE CONSULTING