Convincing C-Suite on Cybersecurity Spend

Webinar Speaker

Aamir Jamil, CISM, CGEIT
Director, GRC Simplified Limited, UK

Aamir is an IT Governance Evangelist. He is helping boards and executive management in ensuring value from IT-enabled investments.

He has had a long and varied career in IT-Governance, digital business transformation, ICT Strategy development, and Information/Cyber Risk Management. He has been described as trusted adviser with strong strategic and analytical skills, and has a track record of guiding businesses through the transformation process and ensuring value in business investments in IT.

The hallmark of his success is through communicating a clear vision, gaining support from stakeholders, and have the team members sing from the same song sheet to push towards the ideal state.

He is active member of ISACA, has served at the board of ISACA Chapters (Karachi, and Muscat), and regularly speaks at various seminars and forums regarding Information Security and IT Governance.

Reach him at aamir.jamil@yahoo.com

AGENDA

- Preparing for the Boardroom
- Security Program Governance
- Progress Monitoring

PREPARING FOR THE BOARDROOM

CONVINCING C-SUITE ON CYBERSECURITY SPEND

CYBERSECURITY: A BUSINESS AND BOARDROOM PRIORITY

Investors and regulators are challenging boards.

Lawyers are discussing corporate directors' liability.

Cyber risk is now the top of board and audit committee agendas.

Cybersecurity is not a problem induced and solved by technology alone.

It's a business risk - more of a human issue, not a technical one.

Leadership need to pay attention to this issue.

WHAT IS AT STAKE?

Intellectual Property Losses

Legal Expenses

Property Losses

Reputational Loss

Time Lost

Administrative Cost

DIRECTORS NEED TO SEE THE BIG PICTURE

Board members are wondering:

- Am I asking the right questions?
- How do I get comfortable?
- Are we doing enough?
- How do I know we are doing the right things?
- Are we making the right decisions?

COMMON DILEMMA

Business executives

"I see what I am being asked to pay, but what value I will get?"

CISO

"The business case I built was comprehensive, but the business executives did not see the value."

CISOs need to learn how to speak the language of business.

CYBERSECURITY IN BUSINESS CONTEXT

Business needs clarity on:

- the degree of strategic alignment,
- the expected tangible and intangible business value
- the level of risk incurred.

Executive management must have a clear understanding of what to expect from their information security program.

SETTING CLEAR EXPECTATIONS

- What are you securing? IT System or Information?
- What are your Crown Jewels?
- What is the Maturity of Cybersecurity?
- Is Security Strategy aligned with organization's business objectives?

SECURITY PROGRAM GOVERNANCE

CONVINCING C-SUITE ON CYBERSECURITY SPEND

SECURITY GOVERNANCE

Security governance is the means by which you control and direct your organization's approach to security.

Security is the responsibility of everyone within the org.

Security decision making can happen at all levels.

Security Governance set out delegation of authority.

WHAT APPROACH IS RIGHT FOR ME?

Answering the following questions will help you decide how formal your approach should be:

- How large and complex is your organization?
- What resources are available for security governance?
- What does your organization do, and how important is security to those aims?
- Are there any external considerations?

WHAT DOES A GOOD APPROACH LOOK LIKE?

Regardless of the level of formality, good governance should:

- clearly link security activities to your organization's goals and priorities
- identify the individuals, at all levels, who are responsible for making security decisions and empower them to do so
- ensure accountability for decisions
- ensure that feedback is provided to decision-makers on the impact of their choices

Approach to security governance should fit into an organization's wider approach to governance.

SECURITY STRATEGY

If you do not know where you are going, you cannot find a way to get there, and will not know if you have arrived.

Determining what needs to be done to move from the ***current*** to the ***desired state*** by using a gap analysis.

Desired State - outcomes set by senior management.

Levels of acceptable risk drive Control Objectives.

CISO determines Security Program

SECURITY PROGRAM

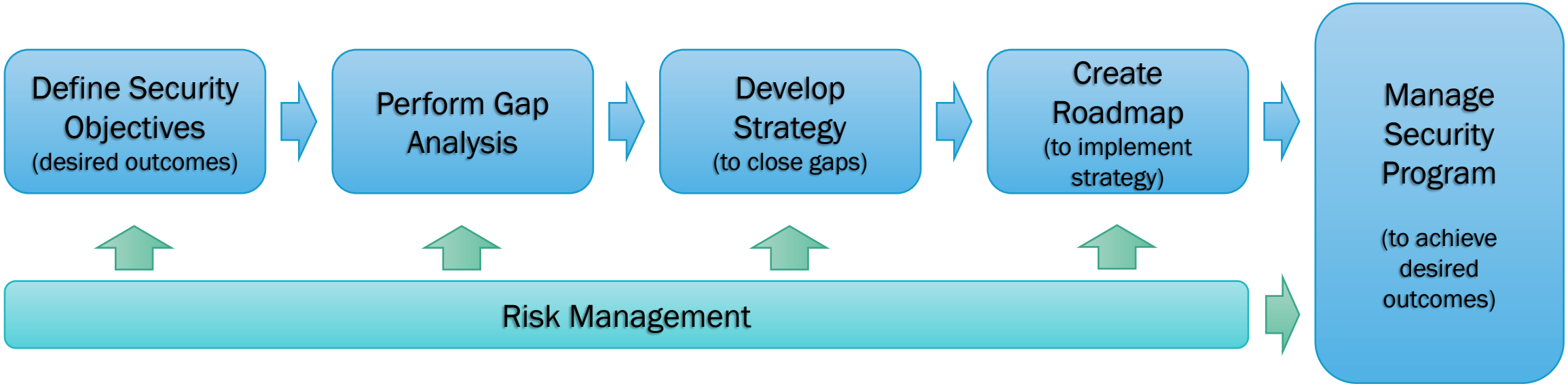
To execute the strategy and achieve the organizational objectives.

Encompasses all activities that serve to provide protection.

Essential Elements of Security Program

- Security Strategy
- Stakeholder Engagement
- Measurement Metrics

SECURITY PROGRAM DEVELOPMENT



PROGRESS MONITORING

CONVINCING C-SUITE ON CYBERSECURITY SPEND

MANAGEMENT WANT MEANINGFUL REPORTS

Does your report look like this?

1M Malicious att

38K Vulnerabil

407 Security Incidents Resolved

Report what you should, not what you can.

Do not present your tools Dashboard

ment on pre-

Report need to update strategy or program

WHAT DOES A GOOD REPORT LOOK LIKE?

An executive management report should contain at minimum the following three sections:

- Explanation of a strategy and security program
- Operational efficiency of a security organization
- Cost of security deliveries

USING RIGHT TOOLS FOR REPORTING

Short-term Tactical Vision	DASHBOARD	Indicators?	How do responsible Managers keep the ship on course?
Long-term Strategic Vision	SCORECARDS	Measures?	How can the enterprise achieve results that are satisfactory for the largest possible segment of stakeholders?
Capability Maturity Model	BENCHMARKS	Scales?	How can the enterprise be adapted in a timely manner to trends and developments in its environment?

WHICH REPORTING TOOL IS APPROPRIATE?

Balanced Scorecards

- Well known to management.
- Position the CISO as a partner.
- Stimulates executive management.

Dashboards

- Maintained at Operational Level
- Control day-to-day operations

Benchmarks

- Assess Current and Desired State
- Justify/Convince Security Spend

CONCLUSION

To convince C-Suite executives on cybersecurity spend, CISOs need to adapt holistic approach.

Insufficient management support is not an issue of apathy, but a lack of clarity.

There may be financial or other reasons for limited support.

CISOs must maximize the effects of available resources.

CISOs should improve communication with C-Suite.

Aamir Jamil, CISM, CGEIT
Director, GRC Simplified Limited, UK

simplified
Governance – Risk – Compliance

Consultants & Trainers

T: +44 (0)20 80501024
E: contact@grcsimplified.co.uk
W: www.grcsimplified.co.uk

Send your questions to: aamir.jamil@yahoo.com