CYBER SECURITY- WITH THE BEST
HTTP://WWW.WITHTHEBEST.COM
15-16 OCT 2017

"A Typical Day in the Life of a CISO"

Abbas Kudrati

Chief Information Security Officer

KPMG- Australia

OVERVIEW

- The security role alphabets
- What do you think CISO does?
- Who should CISO Reports to ?
- The evolving role & future of the CISO
- A Survival kit of skills

THE SECURITY ROLE ALPHABETS

ISO – Information Security Officer

- Often an “IT” Security Officer
- Designated official, dedicated to information security

ISM – Information Security Manager

- Specialize staff with experience in managing team and monitoring security operations
- Experience in Legal, Governance and Compliance Framework

THE SECURITY ROLE ALPHABETS

CISO – Chief Information Security Officer

- "C" level executive, a strategic business partner

CSO – Chief Security Officer

- Corporate security, a convergence of information, asset, and physical security

CHIEF INFORMATION SECURITY OFFICER

JOB DESCRIPTION

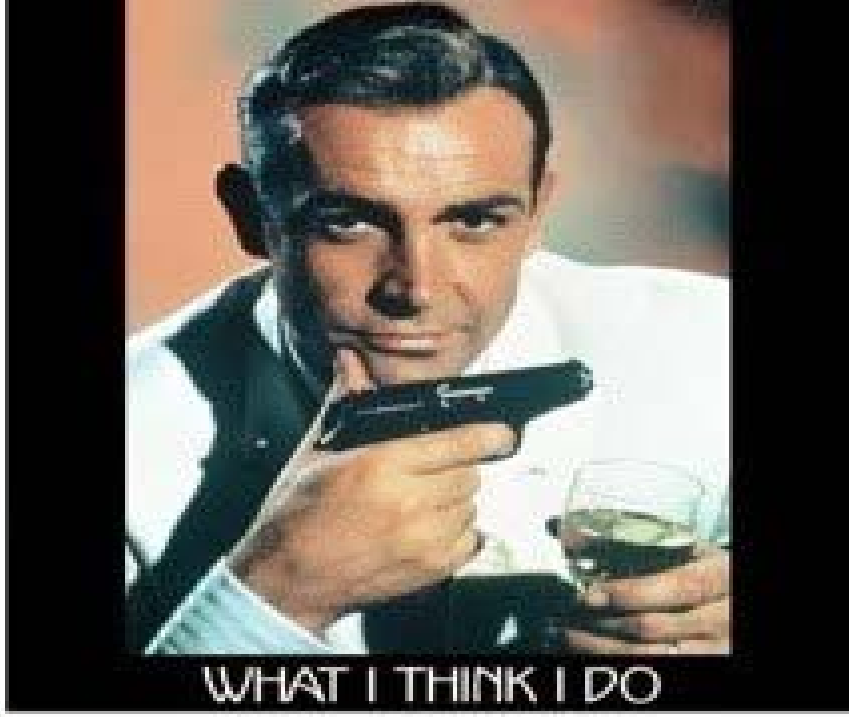
A Chief Information Security Officer (CISO) directs strategy, operations and the budget for the protection of the enterprise information assets and manages that program. The scope of responsibility will encompass communications, applications and infrastructure, including the policies and procedures which apply.

A CISO directs and approves the design of security systems; ensures that disaster recovery and business continuity plans are in place and tested; review and approves security policies, controls and cyber incident response planning; and approves identity and access policies.

SO WHAT DO YOU THINK CISO DO ON A TYPCAL DAY


WHAT MY KIDS THINK I DO


WHAT MY WIFE THINK I DO


WHAT I THINK I DO


WHAT MY FRIENDS THINK I DO


WHAT STRANGERS THINK I DO


WHAT I REALLY DO

CISO INTERFACES

MEETINGS….MEETINGS…..MEETINGS…. & MEETINGS.

"At this point in the meeting we'll open a discussion of whether or not we needed to have this meeting."

MEETINGS BREAKDOWN

Break your meetings down with the **10-30-50-90** rule:

- **10 minutes** for check ins and quick questions.
- **30 minutes** for status updates and one-on-ones.
- **50 minutes** for addressing multiple issues or topics.
- **90 minutes** for brainstorming and problem-solving.

Remember, more meeting time doesn't necessarily mean more progress.


Global SOC emails
Stake holder manage ments
Daily Threat Intel
The Daily Show
Meetings with Vendors
Agile Meetings
Meetings with Peers
Recurrin g meetings


Odds and Ends
Metrics and Reports
Client's query and meeting
Socialize
Networking meetings
Mentoring and Coaching
Research and Conference
Knowledge Upgrade

ENSURE COMMUNICATION PLAN -DELIVERS TARGETED SECURITY MESSAGE

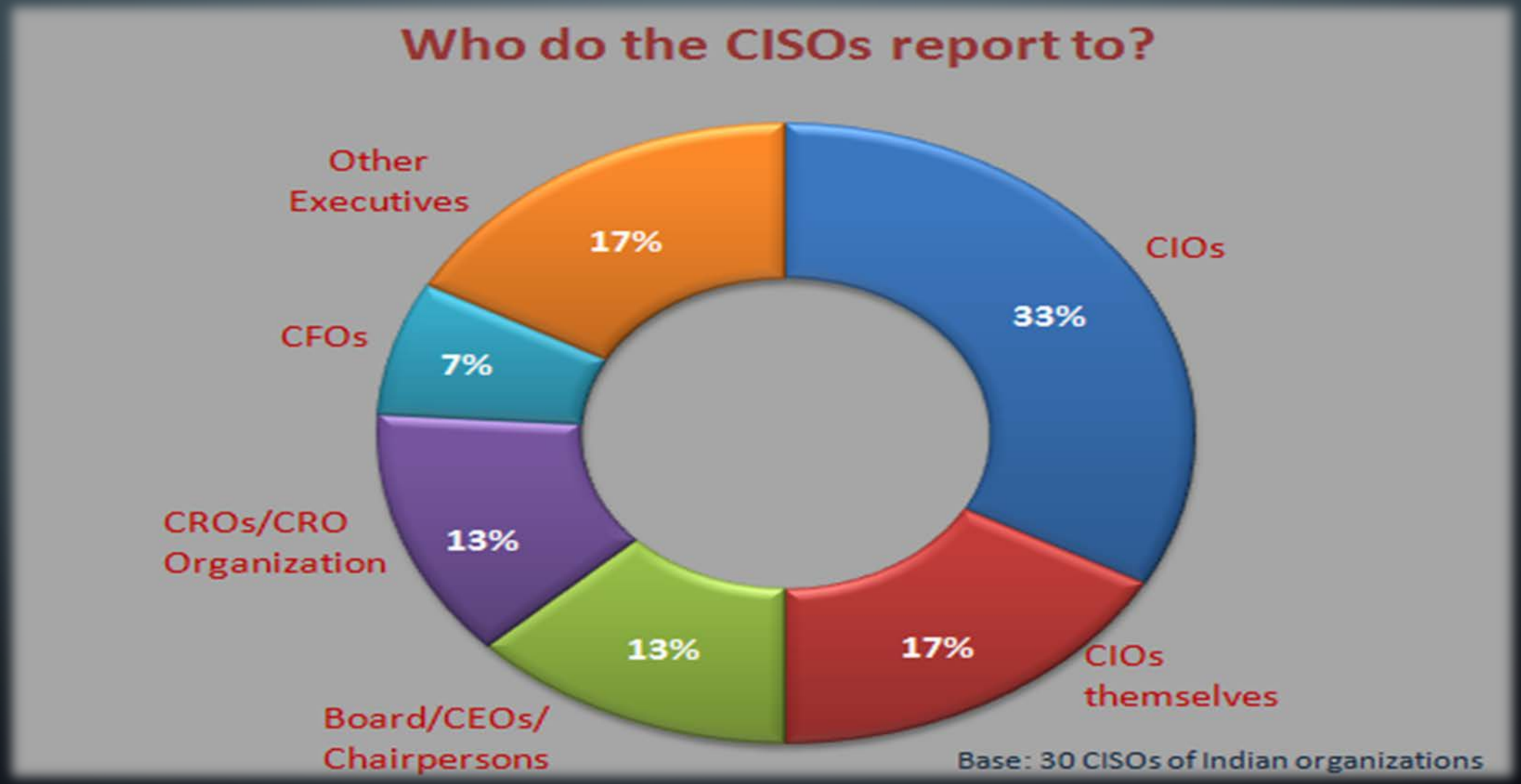
Manager Meetings	• Tactical Plans • New Policies • Scheduled Activities
IT/Business Steering Committees	• Strategic Initiatives • Policy Approval
Board of Director Meetings	• Security Posture • Competitor Comparison
Management, Newsletters,emails	• Interim Updates • Issue Reinforcement
One-On-One Sessions	• Departmental Issues • Testing Reality


And then I said
"We're working quickly to resolve the issue"

THE “DEBATE”

WHO SHOULD CISO REPORT TO?

WHO DO CISO REPORT TO ?



7 REASONS WHY CISO SHOULD NOT REPORT TO CIO

1. Security is an issue for the entire company, not just the IT department. As a CISO advisor said, "A CISO's job is not to protect IT - a CISO's job is to protect the business."

2. Organisations where the CISOs report to CIOs have 14% more downtime due to security incidents, according to a study by PwC.

3. Organisations where the CISO reports to the CIO have financial losses that are 46% higher, according to the same PwC research.

4. If security concerns threatens to stall an IT project, the CIO might overrule it.

5. The CIO might be reluctant to approve security projects that hinder IT productivity.

6. If a security project costs money, the CIO might choose to spend it on IT instead.

7. Some regulators are beginning to mandate CISOs report to the CEO - and many more may follow. In Israel, for example, there are laws dictating that CISOs report directly to the CEO.

http://www.cio.co.uk/it-security/seven-reasons-ciso-should-report-ceo-not-cio-3634350/

REPORTING TO THE CIO - ADVANTAGES

Advantages of reporting to CIO:

- Access to executive leadership
- “C” level skills and organizational awareness
- Ability to initiate change in the IT infrastructure to enhance information security
- Represents greater influence and value for the CIO position

IF INFORMATION SECURITY MOVES OUT OF IT

- Accountability must follow responsibility
  - CIOs do not want accountability without authority
- CISO must report to an executive with “broad managerial responsibilities” for the organization,
  - For example, the CEO, CFO, COO
- Information Security and IT must work closely together as a team.

THE EVOLVING ROLE & FUTURE OF THE CISO

THE FUTURE OF THE CISO A VIEW FROM GARTNER

More companies are appointing a CISO with

"decreasing responsibility for day-to-day security operations, and a greater level of participation in strategic business decisions"

Gartner predicts:

"there will be a new breed of security expert who will be trusted to protect the organisation of the future, and in many companies, this person will be given the title of the Chief Information Security Risk Officer (CISRO)"

THE EMERGING CISO ROLE

- Technical security is becoming an operational issue
- Information security is emerging as a strategic business issue, addressed through risk management processes
- Resulting in “more authority and influence being invested in the security manager or CISO”
  - More CISOs are participating in “crucial business decisions” and are reporting outside of IT
- Ceding turf to a “more powerful security function also raises political issues,” especially with the CIO position.

THE EMERGING CISO ROLE *(CONT')*

- Experts are divided over whether the CIO, CSO, or CISO should be responsible for security
- However, it is clear that the IT industry is moving toward "shared responsibilities for security"
- So, "whether the roles of the CIO and the CISO are mutually exclusive or gradually merging into a mutually beneficial relationships still is not evident."

THE EVOLVING ROLE OF THE CISO

	CISO Role Today	CISO+ Role in Future
CISO's Background	• CISOs come from varied backgrounds • Often inherited the role • Moved up through the IT or business ranks • Some are hired from outside to create public perception	• Proven track record to lead during a crisis • Knows how to take risks • Ability to manage & communicate clearly and concisely to upper management / Board • Heavy on business skills / Lighter on technical skills
Reporting Line	• CISOs typically reports to CIO; typically a layer in between CISO and CIO • Some CISOs report to COO	• CISO+ reports directly to CRO or COO • Have responsibility for; Strategy, Policy, Ops, Compliance, Crisis Management
Level of Authority	• Not always viewed as a key decision maker • Seldom an actual executive role • Often tactical and reactive	• Transformational leader • Sr. level executive • Combined role of IT Risk Officer & CISO • Responsible for Initiatives & Ops • Strategic & pro-active
Areas of spend / Budget responsibility	• Majority of budget directed at maintenance projects to keep current initiatives running • Other spending on pro-active initiatives and reactive projects	• Majority of budget spending will be on transformational initiatives • Budgets should be a percent of the Enterprise budget since all functional groups have security requirements

THE CHANGING ROLE OF THE CISO & DIGITAL TRANSFORMATION

As the business evolves and technology adoption increases with

- IoT (Internet of Things)
- Cognitive computing, Artificial Intelligence
- Industrial Control Systems
- Cloud Computing
- Enterprise Mobility
- Big Data & Analytics

The challenges & interaction of CISO's gets much wider and risks emerge from across different business domains. The security threats today are more organized crime industry and nation-state actors which demand CISO to understand and manage digital technology adoption and transformation with business objectives, a legal and regulatory landscape in mind.

A Survival Kit of Skills for the CISO

A SURVIVAL KIT OF SKILLS FOR THE CISO

- Grounded in multiple protection disciplines
- Capable project/program manager
- Life long passion to learn
- Business acumen
- Diplomatic and adaptable
- Adept at framing issues as risk management
- Professional training and certifications

A SURVIVAL KIT OF SKILLS FOR THE CISO

Connect: Connecting with industry players and peers with similar interest and business risks will allow you to discuss and learn from their success or failures. Also, connecting with cross-industry & cross-continental security leaders will open up new ideas of protection strategies and allow you to be innovative in your security strategies.

Collaborate: CISO networking platforms and security events are good sources to learn about new technologies and most importantly meet other security leaders in person. Peer interactions and deliberation are helpful to gain different perspectives to addressing security risks, it would also allow you better manage your security initiatives by learning different ways of doing same things from different organizations.

Contribute / Share: The power of sharing information is invaluable, the only way, you can beat the adversary is by learning his techniques and actions. This can be more effective as a community that shares information with each other and partnerships from industry service providers. CISO roundtables and other closed-door sessions have also proven to be very effective.

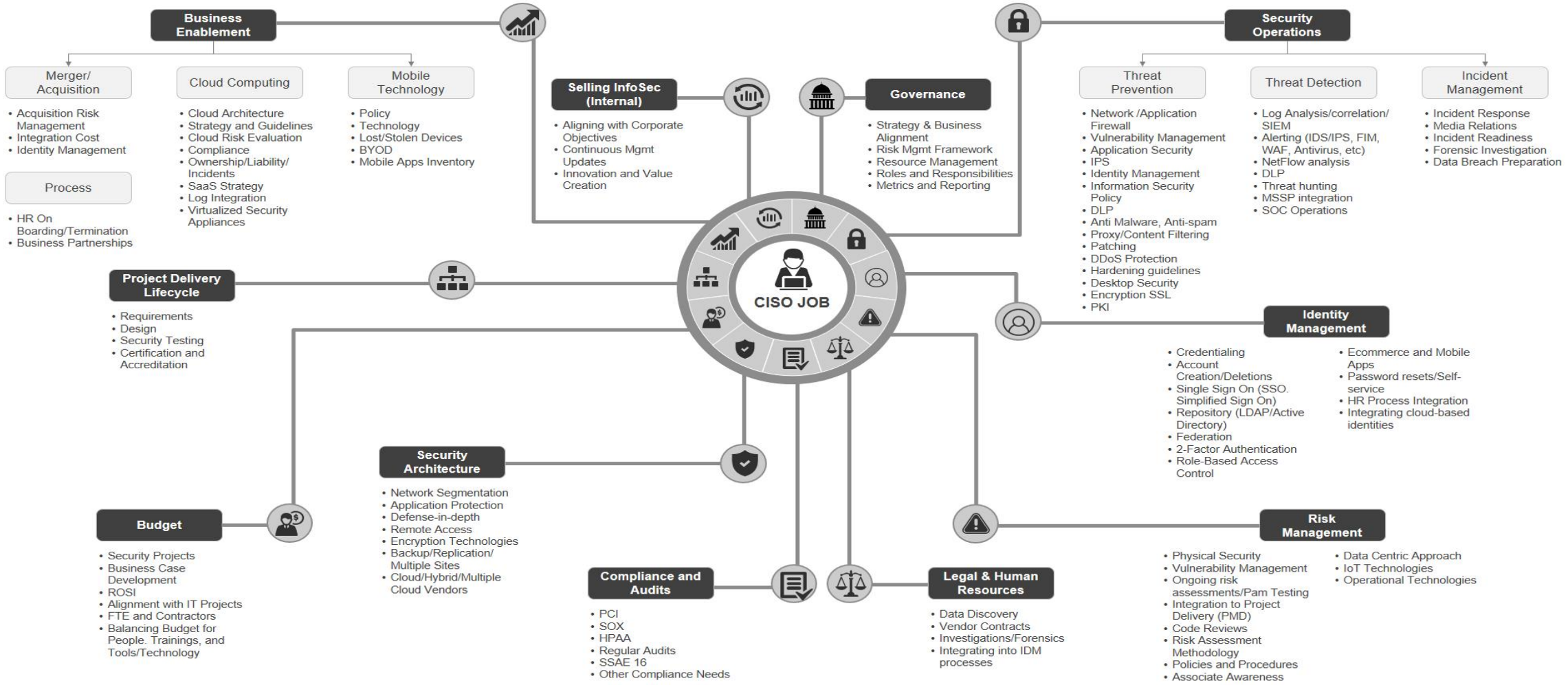
Learn: Learning & professional development should be an integral part of individual growth and way to get familiar with advances in technology and other business practices. The vast experience and knowledge gained by global industry leaders, that is available through books, courses, conferences, and articles will prove to be very helpful against all odds to overcome challenges.

END NOTE – SUCCESS MANTRA

- ✓ **Ensure the C-level execs are confortable with the risk appetite**
- ✓ **Ensure you are comfortable with how you treat risks**
- ✓ **Balance risk and cost**
- ✓ **Run an effective team**
- ✓ **Establish top-notch incident management**
- ✓ **Use resources and knowledge outside your team effectively**
- ✓ **Prioritize works based on risk**
- ✓ **Help your team grow**
- ✓ **Be a servant leader**

CISO Mind Map

Momentum PARTNERS



Source: http://rafeeqrehman.com/2015/05/17/the-latest-2015-ciso-mindmap-is-here/

An Overview of The Responsibilities and Ever Expanding Role of The CISO

SO WHO WANT TO BE A CISO ?

Questions !!!

Abbas Kudrati

https://au.linkedin.com/in/akudrati