Qualities of an Effective CISO

Miguel (Mike) O. Villegas

CISA, CISSP, GSEC, CEH, PCI QSA, PA-QSA

Vice President- K3DES LLC

mike.villegas@k3des.com

November 10, 2015

Abstract

Hiring a Chief Information Security Officer (CISO) is a laudable goal. It implies executive management realizes the value of having an executive level position for information security.

The CISO is an executive who provides expert guidance to other c-level executives on matters of risk, compliance and information protection from a strategic and tactical business objectives perspective. Security practitioners are typically technical in nature but do not generally have access to c-level executives, so the CISO position can help fill in this gap.

This session will discuss the qualities of an effective CISO. This includes education, background, reporting structure, focus, responsibilities, personal qualities, vision, leadership capabilities, and technical background.

Table of Contents

- CISO Resume
- Reporting Structure
- CISO Vision and Responsibilities
- Personal Qualities
- Leadership Qualities

CISO RESUME

CISO Survey

A survey conducted in July 2014, 203 US-based C-level executives found a startling lack of respect for CISOs in the enterprise. Below are some interesting statistics:

- 74 % said they **do not believe CISOs deserve a seat at the table** and should not be part of an organization's leadership team.
- 54 % believe CISOs should not be responsible for cybersecurity purchasing.
- 44 % believe CISOs should be accountable for **any** organizational data breaches.
- 28 % said their CISO has made cybersecurity decisions that negatively impacted the organization's financial health.

Source: http://www.threattracksecurity.com/resources/the-role-of-the-ciso.aspx

CISO Resume

Ideally, a CISO should have a combination of business and technical skills that allow for competent contributions and guidance with both IT and executive management. A successful CISO will be able to incisively translate technical challenges and strategies into business terms. Some specific recommended qualifications for a CISO include:

- Degree in accounting or MBA, degree in CIS or Information Security;
- CPA, CISSP, CISM, CISA, PMP certifications;
- CFE, CEH, GPEN, CRISC specialized certifications;
- Ten years minimum experience as a CISO, information security engineer, or security consultant. Big 4 senior managers or partners from the systems assurance would be an added plus
- ISSA, ISACA, (ISC)^2, OWASP, or CISO forum memberships.

Certifications vs Experience

Many of us have known those that tout technical expertise because of their long list of certifications yet once hired, it does not take long before realization sits in. Hiring a CISO…

- **Certifications** get him through the door.
- The **interview** gives him a seat.
- The **90-day probationary period** assures he can stay
- His **technical abilities** determine what kind of work he can manage
- His **communication skills** determine whether he deserves a "seat at the table" (Board)

Why not hire within?

Security professionals who work within the enterprise have great advantages.

- They know the IT environment
- They know the business
- They have earned certifications that are the envy of many
- They have established a competent rapport with network engineers and system administrators

However, many times the **Peter Principle** might apply such that the security professional has gone as far as he is capable of.

Good CISO Candidates

There will always be exceptions and each candidate should stand on their own. However, below is a list of good candidates for CISO.

- Director of Information Security
- Internal security professionals
- IT Audit Manager
- IT Risk Manager
- External CISO hire
- Big 4 Senior Manager or Partner
- Sr. Security Consultant

A prophet is not accepted in his own country

REPORTING STRUCTURE

Reporting Structure

There are four basic questions in this debate.

(1) Should there be a CISO position?
(2) Who should the CISO report to?
(3) What are the pros and cons for CISO reporting structure?
(4) Who decides?

Should there be a CISO position?

The keys to making the CISO role successful are independence, empowerment and position. The CISO needs to be:

- **Independent** of influence or pressure from those affected in the protection of corporate assets;
- **Empowered** to deploy all proper levels of protection; and
- **Positioned** within the organization to embed information security into the business culture.

Who should the CISO report to?

The survey conducted in July 2014 by ThreatTrackSecurity reported found that:

- 47% of CISOs report to their CEO or president
- 45% report to the CIO,
- 4% to the Chief Compliance Officer, and
- less than 2% to the COO or CFO.

Source: http://www.threattracksecurity.com/resources/the-role-of-the-ciso.aspx

Pros and Cons for CISO Reporting Structure

Pros:

- C-level executive that supports, understands and champions the information security function and CISO
- This provides the CISO independence, ability to disagree and empowerment to deploy the information security program

Cons:

- Where the CISO reports to is situational
- He might lose contact, credibility, cooperation and empowerment to control the security of corporate assets.
- C-level executive does not have sufficient appreciation or influence to support the CISO.
- Conversely, reporting to the CIO could be just as repressive
- It comes down to who the CISO would ultimately report to.

Who decides?

Despite the endless debates and opinions voiced whether the CISO should report to the CIO or another C-level executive, the ultimate question is "Who decides?"

- It clearly will not be the newly hired CISO.
- It will not be the existing Director of Information Security.
- The CIO might recommend hiring a CISO but very likely reporting to the CIO.
- The CEO and board members should ultimately decide but typically the question is not a consideration until they have experienced a breach or a major security incident.

CISO VISION AND RESPONSIBILITIES

CISO Vision and Responsibilities

The CISOs **vision** is to align the information security program with the enterprise strategic business objectives.

The CISOs **responsibility** is to ensure the information security program meets those objectives and grows commensurate with the enterprise goals. Executive management looks to the CISO to:

- Define and manage the information security program
- Provide education and guidance to the executive team
- Present options and information to enable decision making
- Act as an information security advisor

CISO Vision and Responsibilities

This includes, is not limited to:

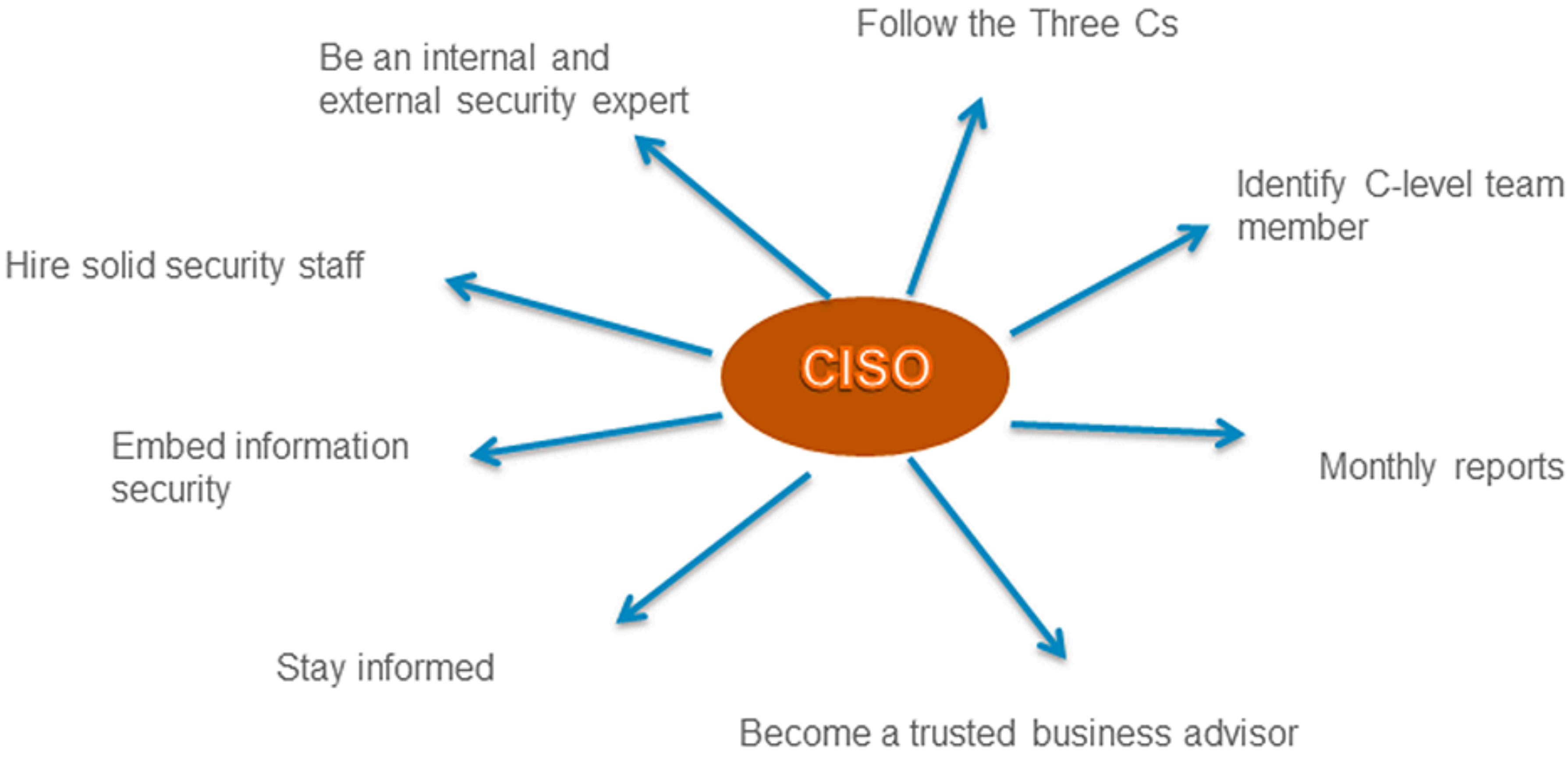
- Executive Management Reporting
- Risk and compliance
- Information Security Administration
- Competent and skilled staff
- CSIRT Program
- Information Protection
- Security Monitoring
- Security Policies and Procedures
- Vendor Security
- Wireless Security
- Mobile Device Security
- Web Application Security
- Vulnerability Testing
- Security Tools
- Network Security
- Application Security
- Personnel Security
- Database Security
- Cloud Security
- Security Awareness Program

What the CISO should do to earn respect

- Use the "three C's" to emphasize the importance of information security within an organization:
  - Cooperation precludes pernicious silos;
  - Communication is critical but it must be incisive, relevant and done with aplomb; and
  - Counterbalance ensures contributions are commensurate with business objectives.
- Identify a C-level team member who can champion the CISO's contributions and participation. Befriend, educate, earn trust and provide him or her with insightful information that will also elevate his or her visibility and credibility.
- Schedule monthly executive management reports on the state of information security for your enterprise. Use graphics, red-yellow-green icons to highlight areas to focus, and communicate your message in business terms related to cost, ROI, risk, growth and compliance.
- Stay informed of current events and new technologies, especially as they relate to your enterprise industry.

What the CISO should do to earn respect

- Give business managers reason to praise your efforts and value. Meet with key business managers to better understand their pain points as it relates to information security, risk and compliance. Be a trusted business advisor.
- Embed information security in the project management cycle, change the management lifecycle and the information governance process.
- Hire or build an exemplary staff with passion for information security.
- Be a luminary in your field so executive management is aware of your endeavors, not only from within, but from others outside your organization. Write articles. Give lectures on information security. Participate in professional organizations to gain insight of what works and what doesn't.
- Use a proven and industry accepted framework, such as ISO-27001 or NIST Cybersecurity Framework (used by Cybersecurity Nexus CSX)



CISO

Follow the Three Cs

Be an internal and external security expert

Identify C-level team member

Hire solid security staff

Monthly reports

Embed information security

Stay informed

Become a trusted business advisor

PERSONAL QUALITIES

Personal Qualities

- Trusted Business Advisor - have a business sense on enterprise strategic goals
- Security Engineer - Technically competent such that he can stand toe-to-toe with IT
- Leader - Leads staff by example
- Manager – manages projects to completion
- Presence - Good presence with executive management demanding attention and respect
- Communicator – ability to communicate technical topics to Board in terms they understand and support
- Assertive – not aggressive; does not have to right or win an argument all the time
- Ethical – does not occult bad news to save face
- Manageable – CISO cannot manage if he is not manageable

Personal Qualities

- CISO needs to be
  - Incisive,
  - Diplomatic, and
  - Confident
- CISO should have high technical acumen
- CISO should be passionate about information security
  - but not so quixotic or dogmatic that it would call their credibility into question
- CISO should be an agent of change
  - Not a cop
  - Not an auditor
- CISO should be tough skinned

LEADERSHIP QUALITIES

Leadership Qualities

- Cybersecurity is predominantly defensive in nature.
- Enterprises are subject to a constant barrage of attacks from inadvertent and advertent unauthorized access by internal and external sources.
- Each day the information security professional is challenged with new attack vectors and exploits.
- It is no wonder how protection measures, monitoring and remediation efforts seem futile and Sisyphean.

The CISO needs to:

- Lead by example
- Develop and grow the staff
- Recognize staff contributions

Lead by Example

- Infect your staff with your passion
- Hire or build exemplary staff that shares your passion for information security
- Let them see your interest, resolve and motive for information security
- Inculcate the maxim of being an agent of change
- Stand for professional ethics in the event the CISO reporting executive instructs otherwise
- Do not instruct staff or IT to only provide auditors and assessors what they ask for and nothing more
  - This says that half truths are OK
  - Staff will feel half truths are OK with CISO
  - Ultimately hurts the enterprise

Develop and Grow the Staff

- There is an abundance of cybersecurity training that is not expensive such as ISACA, ISSA, OWASP or OJT
- assigning special projects to
  - develop or update security policies,
  - security awareness program,
  - incident monitoring and reporting,
  - vulnerability remediation efforts,
  - controls testing,
  - compliance testing, and
  - proof of concepts (POC) for security solutions, whether you purchase them or not
- certification training for
  - CISSP, CISM and CISA
  - SANS courses, E-Council

Recognize Staff Contributions

- Recognize them publicly through
  - newsletters,
  - personally named, when appropriate, in management meetings,
  - allow them to participate in visible projects, and
  - give credit to those that had a direct hand in special project achievements.
- The CISO many times will get all the glory but will also get all the blame. Staff members need to believe the CISO is there to build, protect and champion their efforts.

The dynamics in this approach will realize staff willing to exceed expectations.

Summary

- ❖ CISO Resume
- ❖ Reporting Structure
- ❖ CISO Vision and Responsibilities
- ❖ Personal Qualities
- ❖ Leadership Qualities

BIO

Miguel (Mike) O. Villegas is a Vice President for K3DES LLC. He performs and QA's PCI-DSS and PA-DSS assessments for K3DES clients. He also manages the K3DES ISO/ IEC 27001:2005 program. Mike was previously Director of Information Security at Newegg, Inc. for five years. Mike currently a Contributing Writer for SearchSecurity-TechTarget.

Mike has over 30 years of Information Systems security and IT audit experience. Mike was previously Vice President & Technology Risk Manager for Wells Fargo Services responsible for IT Regulatory Compliance and was previously a partner at Arthur Andersen and Ernst & Young for their information systems security and IS audit groups over a span of nine years. Mike is a CISA, CISSP, GSEC and CEH. He is also a QSA, PA-QSA and ASV as VP for K3DES.

Mike was president of the LA ISACA Chapter during 2010-2012 and president of the SF ISACA Chapter during 2005-2006. He was the SF Fall Conference Co-Chair from 2002–2007 and also served for two years as Vice President on the Board of Directors for ISACA International. Mike has taught CISA review courses for over 18 years.