ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO

And the Confluence of IT Security & Audit

Thomas Borton, MBA, CISA, CISM, CRISC, CISSP
Director, IT Security & Compliance

13 March 2014

AGENDA

1. Introduction

2. Evolution of the CISO: Past, Present & Future

3. Security & Audit: A Confluence

4. Wrap it up

ISACA®
Trust in, and value from, information systems

WHO IS THIS GUY … (BONA FIDES)

Over three decades of physical, material, personnel and information security, Privacy (PII), business continuity and disaster recovery planning experience.

United States Coast Guard, Chief Warrant Officer, Telecommunications (Retired)

Since entering the Private sector, I've worked in the Property and Casualty Insurance and Retail environments where I developed and implemented information security, Business Continuity/Disaster Recovery and Compliance programs.

I wrote, maintain and exercise the IT SOX controls for a $1 billion retailer.

I received my undergraduate degree in business from St. Mary's College of California and my MBA from Dominican University of California.

I hold the following professional certifications:

- CISA (Certified Information Systems Auditor)
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Control)
- CISSP (Certified Information Systems Security Professional)

I am also an instructor for UC Irvine Extended Ed currently teaching a 14-week CompTIA Security+ course

ISACA®
Trust in, and value from, information systems

WHO IS THIS GUY … (BONA FIDES) … BUT WAIT THERE'S MORE …

Affiliation with ISACA

Member of ISACA since 2006 and have been actively involved with ISACA in a variety of senior strategic roles

At the National level:

- Oversight board membership, Knowledge Board – 2 years
  Charge: Ensure the coordination and prioritization of ISACA's professional guidance and knowledge development and dissemination initiatives in support of ISACA's strategy
- Committee co-chair, Knowledge Management and Education Committee – 2 years
  Charge: Identify and support activities to facilitate the management and dissemination of ISACA's intellectual capital and other knowledge assets, inclusive of education opportunities, for ISACA constituents
- Chair, Co-Chair and member of NA CACS (Computer Audit, Control Security) and NA ISRM (Information Security Risk Management) conference task force – 4 years

Local Chapter level

- I serve on SF ISACA's board of directors in the role of research director, maintaining clear communications between ISACA national and international leadership and local chapter leadership

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … A LITTLE HISTORY …

Why security in the first place?

Physical/personal security (historically, safety, both personal, family and community

- security in numbers (communities), weapons, walls, fences, doors, locks, MAD

Personnel Security (background, bodyguards, trust)

Material security (protect food, water, resources, wealth)

- Caveman

Early cities & castles

Information security (where the treasure or resources were kept)

ISACA
Trust in, and value from, information systems

EVOLUTION OF THE CISO … SECURITY NOW OR IN THE NOT-TO-DISTANT FUTURE …

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … LET'S LEVEL-SET, WHAT'S OUT ON THE WEB?

There are many articles (and books) on this topic, just Google *"The Evolution of the CISO"*, to see the list:

- 211,000 results listed
- 2012 and 2013 were big years for opinions on this topic, from sources such as:
  - *IBM*
  - *Infosecurity-magazine*
  - Conferences and seminars
  - *Computerweekly*
  - *CSOonline*
  - *Gartner*
  - Etc …

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … MY STORY, MY EVOLUTION

- My evolution to my current CISO role (1976 through present)
  - "Old-school" security through classroom and on the job training
  - Seminars and conferences
  - Exposure to business processes and requirements
  - Undergraduate and graduate education
  - Audit

- Military (Enlisted)
  - Radioman – classified and unclassified communication systems and data
  - Top Secret clearance
  - Cryptography was part of my day to day operations
  - Classified Material Control Officer (CMCO) – trained and operated a vault
  - Watch officer ashore at a communications station and onboard a CG Law Enforcement cutter
  - Assigned to attend college Duty under Instruction to study computer programming … ugh!
  - Out of college, I built LANs and WANS throughout California
  - Transferred to sole CG mainframe in charge of computer security

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … MY STORY, MY EVOLUTION … THERE'S MORE …

My evolution to CISO role … continued

- Military (Commissioned Officer) Chief Warrant officer, Telecommunications (CWO2 & CWO3)
  - Area Information System Security Officer for:
    - Florida, Georgia, South Carolina, Puerto Rico and the US Virgin Islands
    - California, Oregon, Washington, Alaska, and Hawaii
  - Member of Tiger team that assisted other information system security officers in setting up security and disaster recovery plans for their respective geographical areas
  - Recruited by former Commanding Officer to start up IT Security position at Property Casualty insurance company
  - Went back to college at night to complete my undergraduate degree in business

- 4$ billion privately held Property/Casualty Insurance company (4.5 years)
  - Hired as non-management IT security expert
  - Completed my undergraduate degree in business
  - Began my Graduate degree (MBA)
  - Worked as an international committee member to establish security program and policies for parent multi-national holding company based in Munich, Germany
  - Left company after 4.5 years as Senior Director, IT Security & Disaster Recovery
  - Staff of 17
  - Began studying for CISA

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … MY STORY, MY EVOLUTION … IT WON'T STOP HERE

My evolution to CISO role … almost done

- Retail (just about 10 years)
  - Completed my CISA certification
  - Completed my CISSP certification
  - Completed my MBA, emphasis in Strategic Leadership just before I was hired
  - Hired as IT Manager (matured the position into a IT Director level role)
  - First task was to manage a project writing the IT SOX controls for the company
  - Developed a portfolio of IT security standards, policies, and procedures
  - Completed my CISM and CRISC certifications
  - Established the company business continuity and IT disaster recovery plans and exercise them annually
  - PCI compliance – 3 years running (PCI DSS versions 1.2, 2.0 and eventually 3.0)
  - Privacy compliance, both employee and customer data protection
  - Staff of 1

My role as CISO will continue to grow & evolve as the business grows & evolves

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … OTHER ROADS

Other common (or uncommon) roads to CISO role

- Begin in audit, gain experience, exposed to IT security
- Fresh out of college, audit or security interns, gain experience, jump into a business unit, back to security
- *Tag, you're it …*
- There are many other paths, let's ask the audience …

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … BEFORE THE CISO

Before there were “CISOs”

- There were …
  - Security Conferences (MIS, NIST, ISACA, GARTNER, others)
  - Physical security with specialization in information protection
  - Then in 1995 in the wake of a highly published Russian malware incident, the CISO was “invented”

Steve Katz is widely recognized as the first CISO, he joined Citicorp/Citigroup in 1995 as was appointed to the CISO role there. He later joined Merrill Lynch as their chief information security and privacy officer.

"99% of becoming a CISO was Serendipity and being open to a new career opportunity where there wasn't a career." Steve Katz

- Then came security certifications:
  - CISSP (Certified Information Systems Security Professional)
  - CISM (Certified Information Security Manager)
  - SANS (GIAC - Global Information Assurance Certification)
  - GSLC - Global Security Leadership Certification
  - GISP - Global Information Security Professional
  - Other certs

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … NOW WE HAVE THE “CERTIFIED CHIEF INFORMATION SECURITY OFFICER” C/CISO

Certification body: Electronic Commerce (EC)-Council, from their website;

Description: *”C/CISO will provide your employers with the assurance that as a CISO certified executive leader, you possess the proven knowledge and experience to plan and oversee IS for the entire corporation.”*

Domains:

- *Governance (Policy, Legal & Compliance)*
- *IS Management Controls and Auditing Management*
- *Management – Projects and Operations (Projects, Technology & Operations)*
- *Information Security Core Competencies*
- *Strategic Planning & Finance*

Global reach: over 60 countries, all 7 continents

Wide range of job functions: CISO, CIO, CSO, CEO, Vice President, Chief Security Strategist, Senior IS Director, Chief Security Architect, Senior IT Risk & Compliance Manager

***And coming up next*:** Cybersecurity professionals (Professional development, sunrise to sunset track)

ISACA®
Trust in, and value from, information systems

THE CONFLUENCE OF IT SECURITY AND AUDIT… UNDERSTANDING THE PARTNERSHIP

Security and Audit: A Confluence

Historically there has been a ***tragedy*** and ***comedy*** relationship between audit and security… an “us versus them” … from IT we hear, "the auditors are coming, the auditors are coming" … and from the auditors, "IT just doesn't understand our view of controls and the reasons/methods for testing them.”

Fortunately for security and audit alike, regulations such as GLBA, SOX, PCI, PII, HIPPA have driven IT Security and Audit towards the common goal of effective and sane controls.

More importantly, I believe that these regulations and the requirements to address risk mitigation and relevant controls to company senior leadership and oversight committees have provided the drive to form successful audit/security relationships.

Contentious relationships between auditors and security are not in the best interest of any business.

- Common goals, clear communication and business partnerships are key elements of success

ISACA®
Trust in, and value from, information systems

THE CONFLUENCE OF IT SECURITY AND AUDIT… UNDERSTANDING THE PARTNERSHIP

Security and Audit: A Confluence

My personal experience/my opinon:

Successful CISOs are driven to completely understand all lines of business in their respective company. *Understanding the strategy and contribution of each business unit to the overall success of that business is critical to establishing appropriate security standards, processes, and procedures and the appropriate audit controls.*

As a sole contributor, I find myself moving smoothly between developing, exercising and validating IT SOX controls throughout the year and simultaneously filling the position of CISO with no conflicts. *By necessity I wear multiple hats for security, audit, BCP, disaster recovery, & privacy. Addressing the protection of data and systems from a multi-layered perspective has required me to better understand and assist my business partners.*

I've heard the arguments of, "Well Tom, you know that we can't totally accept your test results and will have test additional samples to show independence." *Understood, I've still reduced the scope of the external audit by providing solid controls that stand up to security and audit requirements and additional testing.*

ISACA®
Trust in, and value from, information systems

THE CONFLUENCE OF IT SECURITY AND AUDIT… UNDERSTANDING THE PARTNERSHIP

Security and Audit: A Confluence

I did spend a fair amount of time up front explaining the evolution of the CISO and my own evolution in particular because I've lived the confluence of IT security and audit. A few closing comments:

- On my journey I've had a few "aha" moments concerning business that I will share:
  - CIO capital cost/ongoing expense versus paying the penalty, and
  - The two sides of the coin, the two different views of the same control: security and *audit*
  - The real customer, our business partners
- Business continuity is a great tool to improve your ability to function as an interpreter & advocate between business, IT and audit (up, down lateral … all directions)

My professional success has relied in large part on my understanding of audit and security and that the business is the driver and beneficiary of both disciplines.

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO AND THE CONFLUENCE OF IT SECURITY AND AUDIT… AND NOW A WORD (OR WORDS) FROM OUR AUDIENCE

Questions/comments from the audience

Your personal experience/opinon's will be of great value to the other attendees,

So please speak up

(or I will be forced to come down among you armed with a microphone)

.

ISACA®
Trust in, and value from, information systems

EVOLUTION OF THE CISO … THANK YOU!

Thank you!

tom.borton@cpwm.com

.

ISACA®
Trust in, and value from, information systems