A Day in the Life of a CISO

Presented by:
Richard Greenberg, CISSP
Information Security Officer
ISSA International Honor Roll
President, ISSA-LA
President, OWASP-LA

The Chief Information Security Officer

- The average U.S.-based CISO now makes $273,033 per year
- There is a severe shortage of qualified individuals
- The average life span of a CISO is 18 months
- Some say CISO stands for Chief Information Scapegoat Officer

A Primer for Up and Coming CISOs

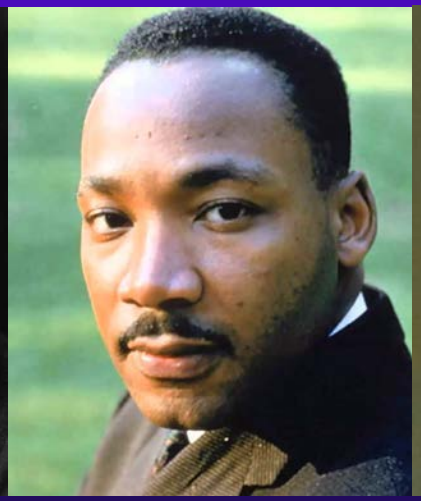
WARNING!

There is still time to consider other careers

But then again, why?

If you embrace challenges, have multiple skills, have business acumen, and love change, YOU may become a great leader.






Step Into the Roll of a CISO for a Day

Virtually and theoretically, that is.

Join me as we explore the variety of knowledge, skills and challenges that must effectively mesh to make you successful

Grab Some Popcorn and Get Comfortable

5:45 AM

- **Check Emails:**

6:15 AM

7:00 AM

- Conference call with CISO of company proposing to host our new web application
  - Discuss their security controls
  - Review contract language
  - Discuss their third party assessments

7:30 AM

Drive Daughter to School

7:35 AM

Risk Assessment

- Will there be more traffic on the Freeway or streets?
  - Each day of the week has a general pattern
  - People in LA hate getting up without the sun, so overcast days are good for the freeway
  - Should I pass that joker who keeps changing lanes?

8:00 AM

Conference Call

- Discuss with consultant why web application vulnerability scan engine stopped prematurely
  - Turns out it was waiting for input
  - It was looking for an external page that wasn't in the test environment
  - These tools cannot be run out of the box; they need configuration.

8:30 AM

- **Arrive at the Office**

8:35 AM

- **Respond to notification of a possible phishing attack**
  - Request forwarding, as an attachment, of suspicious email
  - Analyze url links, headers, sender address, business need or applicability
  - Any attachments? If yes, filter through Virus Total or other reliable online tool
  - If malicious, check logs for user activity and interview user

9:00 AM

- **Discussion with CTO about Identity and Access Management Project**
  - **Have we inventoried all of the applications in the Enterprise?**
  - **Have we identified all the apps that are not synched with AD?**
    - **What are the system access workflows for these apps?**

9:30 AM

- Meet with Head of Application Development
  - Continue review of security requirements for all web apps
    - Passwords: Do we need upper case, lower case, special characters, and numbers, OR only 3 out of 4?
    - Problem with the Captcha: using man-in-the-middle tool, appearing as text
    - Are secure ESAPI libraries being used?

10:30 AM

- Meeting with Chief Privacy Officer
  - Review of Privacy Policies to coordinate and be in synch with InfoSec Policies
  - Ensure compliance with HITECH Act
    - Required HIPAA training and awareness activities
    - Notifications of incidents
    - Encryption of sensitive e-mails

Stream of Consciousness

- CISOs need to keep up with regulations and industry standards
- Regulations tend to trail behind technological innovations
- Don’t rely solely on regulations to secure your environment
- Some example of US regulations:
  - PCI DSS, or Payment Card Industry Data Security Standard
  - SOX or the Sarbanes-Oxley Act
  - GLBA or the Gramm–Leach–Bliley Act

11:30 AM

- Conference Call to Plan Security Awareness Event
  - Events 3x/yr
  - Audience: all staff
  - Invite speakers, such as from LA District Attorney, FBI, Dept of Homeland Security
  - Give-aways and prizes
  - Topics include: ID Theft, Medical ID Theft, Protecting Your Kids On-line

12:15 PM

- Review of Change Management Module in HelpDesk Software
  - To ensure process flow adheres to Change Management Standard and Procedure
  - To ensure all changes to information systems proceed through a formalized process, including ample approvals and testing

2 PM

Lunch and Review of Emails

2:30 PM

- Meeting with App Dev team
  - Web Application Static Security Scanner
    - Scans uncompiled source code of web apps
    - Integrates into the SDLC and assists developers and programmers
    - Identifies insecure code

2:35, 2:45, 2:55, 3:05, 3:15, 3:30PM

- Field unsolicited calls from vendors who have marvelous new products that:
  - make all our environments secure
  - and save me $1M
  - save the world

3:30 PM

- Meeting with System Admins Regarding Security Vulnerability reports
  - Identify repeat offenders
  - Identify clients without successful installation of path management agents and anti-malware agents

4:30 PM

- Review results of Web Application Dynamic Security Scans
  - XXS (Cross site scripting) vulnerability
  - Weak Captcha solution
  - Input validation problems

5 PM

- Meet with Executive Management regarding proposed web app that will have an Internet front end
  - Clinicians will enter patient information from clinics
  - Doctors will be able to log in to see patient records
  - Who else will need access? From where? On what devices/systems? Where will the data be stored?

6 PM

- Meet with CFO and COO to try to secure budget
  - Presentation on the increase in cyber risk to the company
  - Convincing C-Suite that ownership of risk needs to be at their level
  - Try to build a culture of security awareness throughout the organization
- Success! Budget approved!

6:30 PM

- **Conference call about ISSA-LA 9th Annual Security Summit May 19, 2017 at Universal City Hilton**

Key Parting Concepts

- RISK Management
- Reporting structure challenges
- CISO Backgrounds
- Relationships
- Business knowledge
- Salesmanship
- Get management training
- Speak “businessese”

Risk Management

- Most middle to large organizations take risk very seriously
- Often Risk management is at the C-table
- We need to make sure we manage risks so that we minimize their threats but maximize their potential
- Risk is inherent in almost everything we do

Reporting Structure Challenges

- Where does the CISO fit hierarchally in the organization?
  - Most report to the CIO
  - Some report to Risk Management
  - Some report to the CFO
  - Some report to the C-Suite
- Some are CISOs of business divisions and have a fair amount of autonomy from the corporate CISO

CISO Backgrounds

- Most CISOs do not have business backgrounds
- Most have come from technology backgrounds
- Most do not have web application development backgrounds

Relationships

- Take the key decision makers out to lunch
- Make friends with your peers in other divisions
- Support others
- RESPECT
- Know who to go to, to get answers
- Know thine enemies well

Business knowledge

- Learn the business of the company you are in
- Learn what each of the business units do
- Learn the regulatory environment
- Know where the most important information resides

Salesmanship

- Spread a culture of security in your organization
- Identify what is important to each business leader
- Learn the culture of the organization and work within it
- Be creative as you “sell” security

Get Management Training

- **Learn:**
  - **The tools required to lead effectively at the Enterprise level**
  - **How to develop effective, clear innovative strategies**
  - **How to inspire and lead a team**
  - **How to develop a good communications strategy**
  - **Enterprise Security Governance**

Speak “Businessese”

- Executive management will not learn security
- You must learn how to frame your discussions and points in business terms
- Learn what is most important to the C-Suite
- Present your points strategically
- Align and present your goals with the business goals

Q & A

THANK YOU