Beyond Checking the Box

Veryl White
CISA, CISM, CRISC, CISSP
MBA, MS Cyber-Security

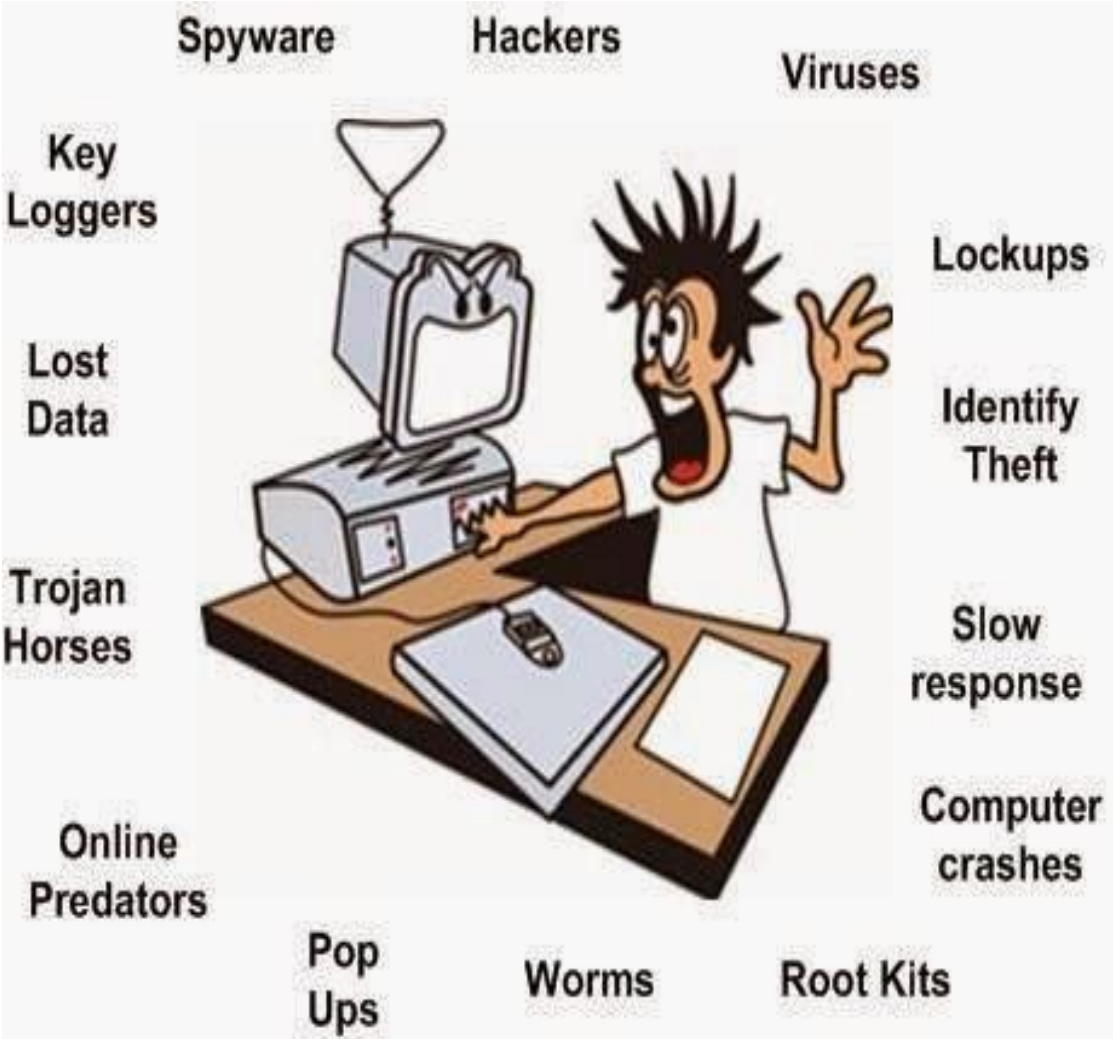
Who I am and What I do

Veryl White, CISSP, CISA, CISM, CRISC, MBA, MS Cyber-Security

The Information Security Manager for a regional retailer with operations in eight states. Prior to this role, I was the Director of Information Technology, responsible for providing the strategic and operational leadership that established, supported and continuously improved information technology strategies.

I attempt to stay current with business and cyber security issues by teaching business and IT courses at several colleges and universities. I have participated in the development of the Florida Teachers Competency exams for Florida K-12 STEM programs. Working with the Florida Department of Education on curriculum committee that developed the Cyber-Security curriculum which was adopted by NIST. I worked with the University of Texas assisting in the development of a new Cybersecurity program .

This is me on a Good Day



Disclaimer

- I disavow any notion that the work I do in Cyber-Security is directed at the protection of enterprise assets. My job is to demonstrate how assets can be attacked with the hope that the cyber-battlefield can be controlled elegantly enough to be able to facilitate a response to all attacks in an effective and adequate fashion.

Compliance

- To act or be in accordance with wishes, request, demands, requirements, conditions, etc.
- Certification or confirmation that the doer of an actions meets the minimum requirements or accepted practices, legislation, prescribed rules and regulations, specified standards or terms of a contract.
- To follow a rule or order.

Security

- The state of being free from danger, risk or threats
- Something that secures or makes safe; protection; defense " *the measures taken to guard against espionage, sabotage, crime, attack, or escape".*
- Precautions taken to guard against crime, attack, sabotage, espionage, etc.

Mediocrity

- To be merely adequate or average, to be just halfway to the highest point of excellence.
- Ponemon Institute declared “2014: A Year of Mega Breaches”

(https://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL3.pdf)

Does this Sound Familiar?

- Security is failing to protect us
- Compliance is just another name for **nuisance**
- Next-Gen security products are not working
- Hackers are getting smarter, bolder, better organized
- Tired of FUD
  - Reports, metrics, assessments that make no sense

Is There Any HOPE?

Even the Empire Failed Compliance

- Key controls were not secured
- Strong Authentication and Access Control
- Incident response planning

Checklists What do They do?

- Improve consistency
- Provide predictability
- Provide organization
- Motivation
- Productivity
- Excellence

Types of Checklist

A list of things to be checked or done

- Grocery List
- To-Do List
- Goals List
- Security Checklists
- Compliance Checklist
- Pre-Flight Checklist
- Surgical Checklist

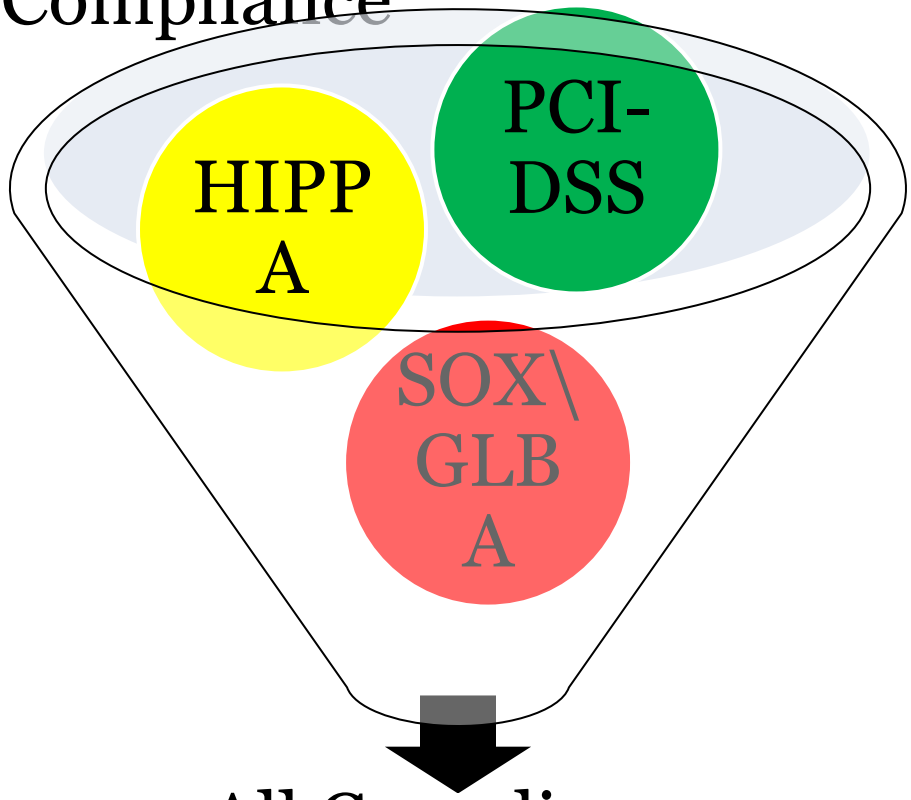
Why Did We Start Checking Boxes

- When did Compliance and Security become a checkbox
  - When organizations realized that compliance requirements were risk based.
  - **Doing more than the bare minimum to comply with the law can be interpreted as being financially irresponsible.**

Trust

- Does filling in the Checkbox instill confidence in your Cyber-Security/Compliance program?

Sorting out Compliance



All Compliance Requirements lead to Security

PCI-DSS Compliant is Simple Right

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain and Information Security Policy

The Challenge

- Creating effective Security Program?
- Do we have one?

  Does it work?

Strategy

- Organizations need to extract the benefits of both compliance and security and focus on protection.

Compliance ≠ Security

Security ≠ Compliance

Security & Compliance

- Using a combination of Security and Compliance is the preferred manner in which to protect your organization from RISK
- What drives security?
  - Compliance
- What funds security?
  - Compliance

Substitute Child-Proofing for Security/Compliance

- Risk Assessment
- House Rules
- Training/education
- Testing
- Monitoring
- Maintenance

Compliance and Child Proofing

- Proactive
- Good Controls (Think before your do)
- Being aware (Training)
- Good Habits (Compliance)
- Tools
- Hard Work and Tolerance

Is good ever good enough?

Talk Threat, Likelihood and Impact

- Do
  - Focus on threats
    - Categorize threats
- Do not
  - Focus on threat actors or products

Security Not Compliance

- How can we satisfy Security and Compliance
- Neither security or compliance can stand alone by themselves

What Constitutes Good Security?

- Governance
- Risk
- Compliance
- Availability
- Accessibility
- Accountability

Conclusion

- Strength does not win, agility does.
- Technology does not protect you, It is how effectively you use that technology.
- Assurance does not come from compliance it comes from governance.
- It is not what you know that is important, it is that you know what you don’t know that is.
- Skill does not make you qualified, character does.

Additional Resources

- NIST SP 800-53r4 Security and Privacy Controls for Federal Information Systems and Organizations

https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet

https://www.sans.org/score/checklists

https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf