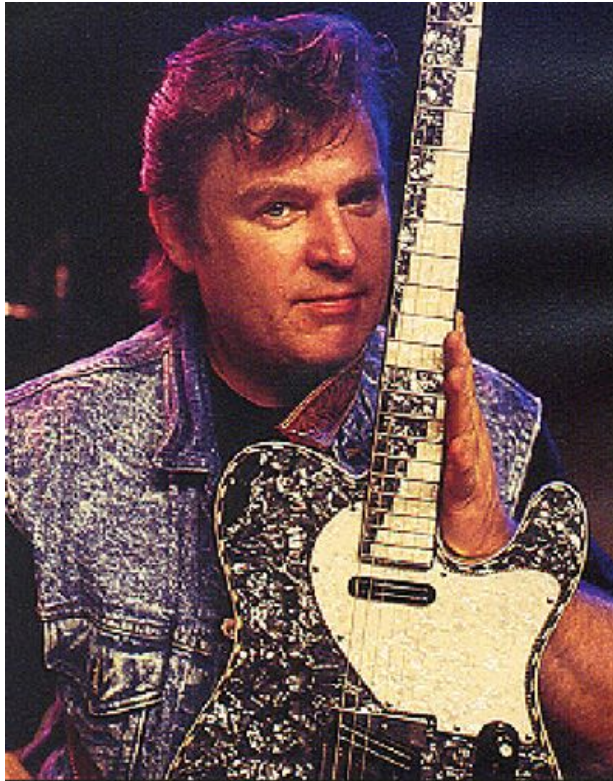




Can you see the dashes along the side?

Sound Check



Daniel Wood Gattton Jr.
(September 4, 1945 – October 4, 1994)



Cruisin' Deuces



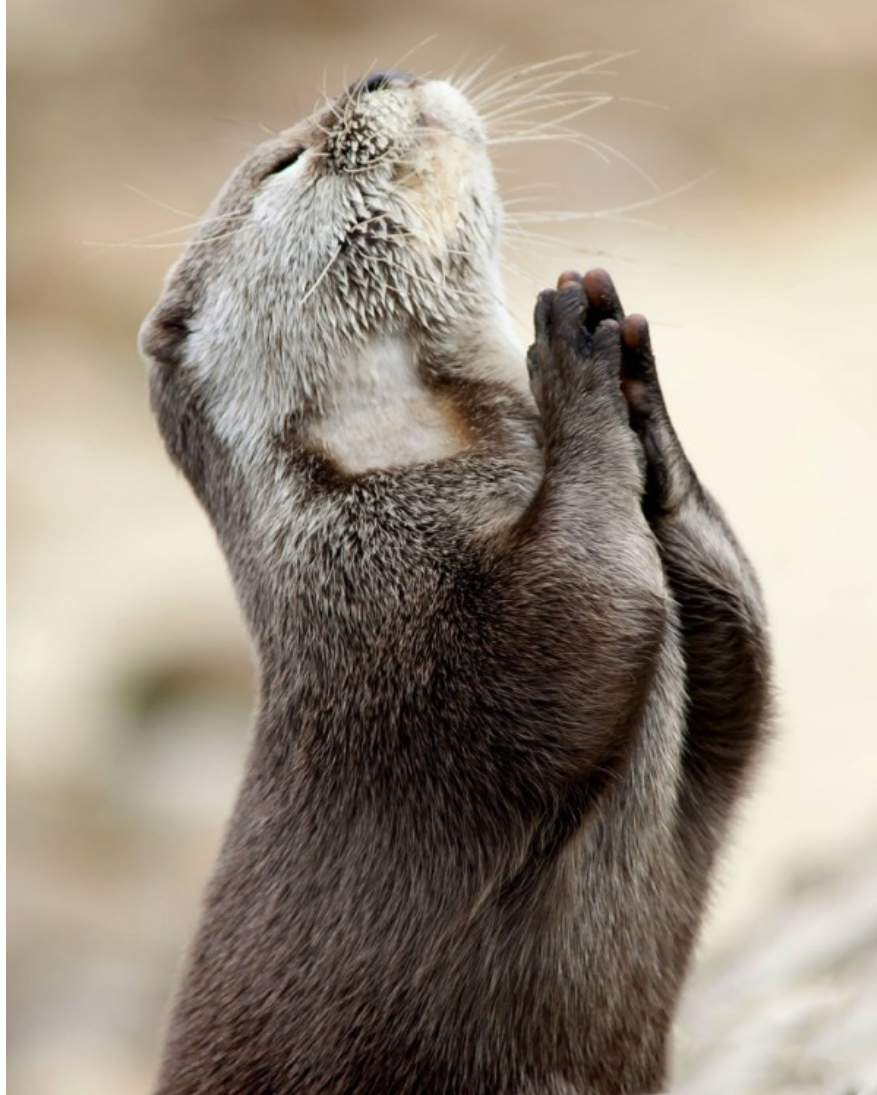
Test Movie Sound Level



For Want of a Patch

Why are you protecting it and what are you protecting.

Please everything work...



Ty Shipman

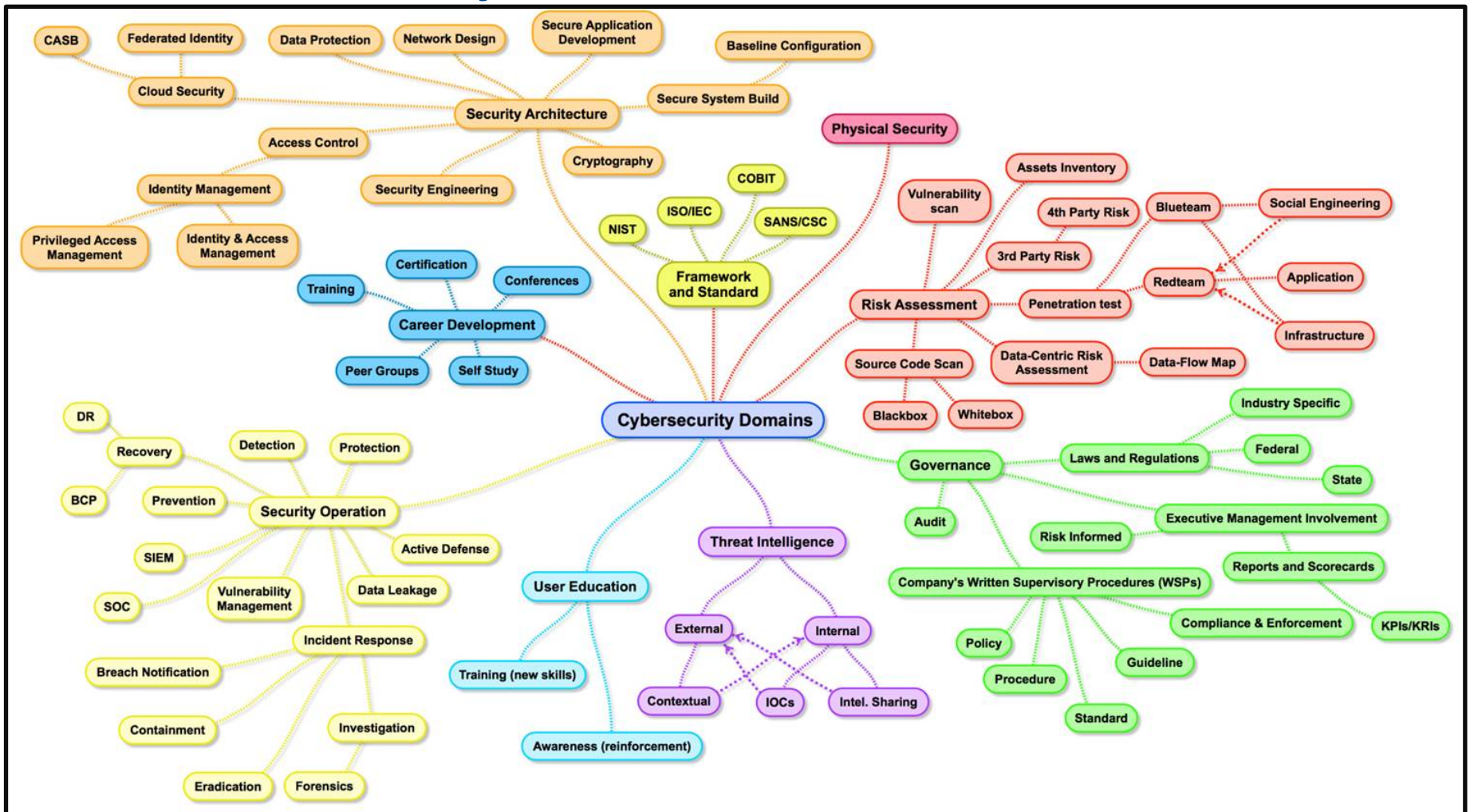
ty.shipman@owasp.org

- <https://www.linkedin.com/in/tyshipman/>
- CompliancePoint
 - Sr. Security Consultant
 - PCI, NIST, HIPPA, SOC2 audits,
 - Network security, PEN testing,
 - GDPR, GAP analysis
- Experience: E-commerce, M-Commerce, IT, Security, Compliance and DevOps
- My past -- Kagi, LoopPay, SamsungPay Labs, multiple patents, and lots of consulting



- Master scuba diver, CISSP, father of 2 amazing kids

Where do you start?



Creator unknown – someone sent this to me.

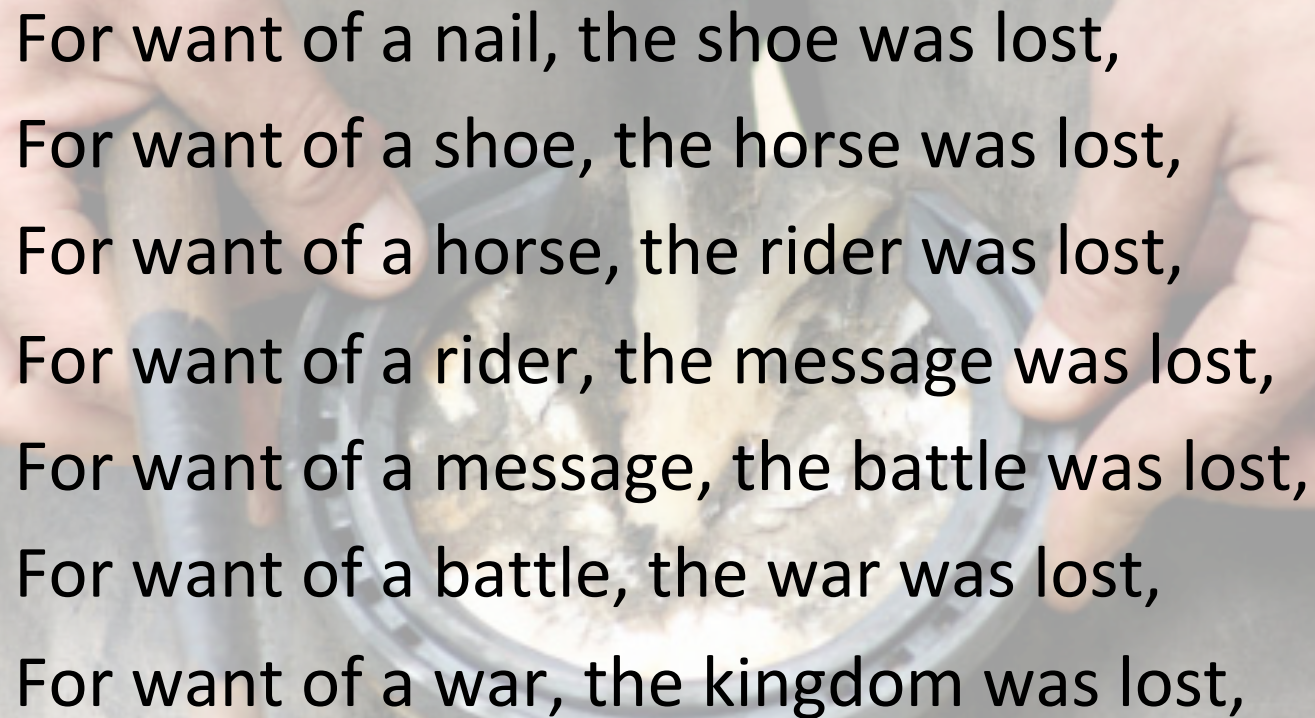
Audience Participation

- Who is in my audience?
- Participation would be nice, win prizes ...

For Want of a Patch - Goals

- Foster better security implementations (postures) through understanding the why.
- Facilitate a framework to better understand why you are protecting your infrastructure.

Old Proverb -- For Want of a Nail



For want of a nail, the shoe was lost,
For want of a shoe, the horse was lost,
For want of a horse, the rider was lost,
For want of a rider, the message was lost,
For want of a message, the battle was lost,
For want of a battle, the war was lost,
For want of a war, the kingdom was lost,

Tokyo Drift -- For Want of a Nail



Fast and Furious – Tokyo Drift
© Universal Pictures 2015

Sonny Chiba as “Uncle Kamata”

<https://www.youtube.com/watch?v=6avCeoDqXSs>

For Want of a Patch

For want of an patch, the application was lost.
For want of a application, the host was lost.
For want of a host, the segment was lost.
For want of a segment, the network was lost.
For want of a network, the data server was lost.
For want of a data server, the critical data was lost.
For the loss of the critical data, the company was lost.

And all for the want of an application patch.

Security Standards

Framework Standards

- BS 7799
- BISA
- High Trust
- Fed Ramp



Prescriptive Standards

- PCI DSS



What are you protecting

Stanza	Protected Class
For want of a patch, the application was lost.	Application
For want of an application, the host was lost.	Host , Guest, Device, Container, Service
For want of a host, the segment was lost.	Segment , VLAN, Subnet, Category
For want of a segment, the network was lost.	Network
For want of a network, the data server was lost.	Host (a specific one at that)
For want of a data server, the critical data was lost.	Data
For the loss of the critical data, the company was lost.	Company, Client, Consumer, your job

PCI DSS – A Good Place to Start

- **Payment Card Industry (PCI)**
 - **Data Security Standard (DSS)**
- Open Loop Credit Card Industry
- Other communities adopting
- CDE – Card Data Environment
 - Critical Data Environment
- CHD – Card Holder Data (Stuff on the card)
 - Critically Held Data (PCI, HIPAA, GDPR)
- Merchant (Level 1-4), Service Provider (L-1), Issuer (L-1)
 - Your deployment



PCI – 12 Requirements, ~242 controls



- 1. Install and maintain a firewall configuration to protect CHD
- 2. Do not use vendor-supplied defaults for system passwords and other security parameters
- 3. Protect stored CHD data
- 4. Encrypt transmission of CHD across open, public networks
- 5. Use and regularly update anti-virus software or programs
- 6. Develop and maintain secure systems and applications
- 7. Restrict access to CHD by business need to know
- 8. Assign a unique ID to each person with computer access
- 9. Restrict physical access to CHD and CDE
- 10. Track and monitor all access to network resources and CHD
- 11. Regularly test security systems and processes
- 12. Maintain a policy that addresses information security for all personnel

And so begins our exploration

Requirement/Control	Protection Class (Application, Host, Segment, Network, Data, Company)
1. Install and maintain a firewall configuration to protect CHD	Segment, Network, Application
2. Do not use vendor-supplied defaults for system passwords and other security parameters	Application, Host, Network
3. Protect stored CHD data	Data
4. Encrypt transmission of CHD across open, public networks	Data, Application, Host
5. Use and regularly update anti-virus software or programs	Application, Host, Network
6. Develop and maintain secure systems and applications	Application, Host, Network

And so begins our exploration #2

Requirement/Control	Protection Class (Application, Host, Segment, Network, Data, Company)
7. Restrict access to CHD by business need to know	Data, Company, Consumer
8. Assign a unique ID to each person with computer access	Host, Network, Data, Company
9. Restrict physical access to CHD and CDE	Data, Company
10. Track and monitor all access to network resources and CHD	Data, Company
11. Regularly test security systems and processes	Application, Host, Network, Data, Company
12. Maintain a policy that addresses information security for all personnel	Company

Testing the PCI DSS Controls

***1.1.2** Current network diagram that identifies all connections between the CDE and other networks, including any wireless networks

Application, Host, Data

2.1.1 For wireless environments connected to the CDE or transmitting CHD, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.

Segment, Network, Host

***12.2** Implement a risk-assessment process that:

- Is performed at least annually and upon significant changes to the environment
- Identifies critical assets, threats, and vulnerabilities, and
- Results in a formal, documented analysis of risk.

Host, Segment, Network, Data, Company

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

2.4 Maintain an inventory of **system components** that are in scope.

*Shred, incinerate, or pulp hard-copy materials so that CHD cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.

***3.1** Keep CHD storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all (CHD) storage:

- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements
- Specific retention requirements for CHD
- Processes for secure deletion of data when no longer needed
- A quarterly process for identifying and securely deleting stored CHD that exceeds defined retention.

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

4.1 Use strong cryptography and security protocols to safeguard sensitive CHD a during transmission over open, public networks, including the following:

- Only trusted keys and certificates are accepted.
- The protocol in use only supports secure versions or configurations.
- The encryption strength is appropriate for the encryption methodology in use.

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

5.2 Ensure that all anti-virus mechanisms are maintained as follows:

- Are kept current,
- Perform periodic scans
- Generate audit logs which are retained per PCI DSS Requirement 10.7.

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information ,and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.

6.4 Follow change control processes and procedures for all changes to system components.

6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.

6.5.6 All “high risk” vulnerabilities identified in the vulnerability identification process.

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.

8.2.3 Passwords/passphrases must meet the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:

- Generic user IDs are disabled or removed.
- Shared user IDs do not exist for system administration and other critical functions.
- Shared and generic user IDs are not used to administer any system components.

9.5 Physically secure all media.

10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls...

11.1 Implement processes to test for the presence of wireless access points(802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.

11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network(such as new system component installations, changes in network topology, firewall rule modifications,

Application, Host, Segment, Network, Data, Company/Customer

Testing the PCI DSS Controls....

11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.

12.1 Establish, publish, maintain, and disseminate a security policy.

11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.

Application, Host, Segment, Network, Data, Company/Customer

Where should you start?

PCI DSS Prioritized-Approach

A	B
PCI DSS Requirements v3.2	Milestone
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	
1.1 Establish and implement firewall and router configuration standards that include the following:	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2
1.1.5 Description of groups, roles, and responsibilities for management of network components	6
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2
1.1.7 Requirement to review firewall and router rule sets at least every six months	6
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	
<i>Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.</i>	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2
1.2.2 Secure and synchronize router configuration files.	2
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	2
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	

Questions and Feedback

- ty.shipman@owasp.org
- Questions?

URL References

- https://en.wikipedia.org/wiki/For_Want_of_a_Nail
- https://www.pcisecuritystandards.org/document_library
 - https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf
- <https://www.linkedin.com/in/tyshipman/>
 - Look in the Publications Section for this talk and others
- <https://pciguru.wordpress.com/>

Ty Shipman

ty.shipman@owasp.org

- <https://www.linkedin.com/in/tyshipman/>
- CompliancePoint
 - Sr. Security Consultant
 - PCI, NIST, HIPPA, SOC2 audits,
 - Network security, PEN testing,
 - GDPR, GAP analysis
- Experience: E-commerce, M-Commerce, IT, Security, Compliance and DevOps
- My past -- Kagi, LoopPay, SamsungPay Labs, multiple patents, and lots of consulting



- Master scuba diver, CISSP, father of 2 amazing kids