REDHAWK NETWORK SECURITY, LLC PRESENTS:

PCI COMPLIANCE FOR THE SMALL BUSINESS

ABOUT TYLER HARDISON

- First Programming Experience 1981, Commodore VIC-20
- 20+ Year Technology Veteran
- 12 Year Veteran in Financial Services

- CISSP
- PCI-QSA
- Currently, Director of Solutions and Innovation Redhawk Network Security, LLC
  Bend, OR

COMMON ACRONYMS

- PCI - Payment Card Industry
- CDE - Cardholder Data Environment
- QSA - Qualified Security Assessor

- Some Disclaimers:
    - This is a high level overview of the PCI Standard
    - Concepts presented here are not endorsed by the PCI council
    - Compliance is a journey, not a destination

PCI 101

WHO IS THIS COUNCIL?

THE PCI COUNCIL

- Initially, each of the 5 major brands had their own standard.
- In 2004, the 5 brands agreed to create the PCI Security Standards Council
- In December 2004, version 1.0 of the standard was released.
- As of 2017, version 3.2 is available.
- The Council provides oversight and maintenance of the Standard, not enforcement

THE PCI STANDARD (10,000FT)

CONTROL OBJECTIVE	REQUIREMENTS
BUILD AND MAINTAIN A SECURE NETWORK	1 Install and maintain a firewall configuration to protect cardholder data 2 Do not use vendor-supplied defaults for system passwords and other security parameters
PROTECT CARDHOLDER DATA	3 Protect stored cardholder data 4 Encrypt transmission of cardholder data across open, public networks
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	5 Use and regularly update anti-virus software 6 Develop and maintain secure systems and applications
IMPLEMENT STRONG ACCESS CONTROL MEASURES	7 Restrict access to cardholder data by business need-to-know 8 Assign a unique ID to each person with computer access 9 Restrict physical access to cardholder data
REGULARLY MONITOR AND TEST NETWORKS	10 Track and monitor all access to network resources and cardholder data 11 Regularly test security systems and processes
MAINTAIN AN INFORMATION SECURITY POLICY	12 Maintain a policy that addresses information security for all personnel

SEEMS SIMPLE, RIGHT?

- 220+ Sub requirements (and growing)
- Some requirements are "intentionally vague"
- Interpretation is often subjective, no two QSAs will agree 100%
- Strategies for compliance are in "guidance" docs
    - https://goo.gl/i4krvJ - Documentation Library

THE DARK SIDE

- PCI QSA Companies who give "false" Reports of Compliance (ROCs)
- Plethora of non-QSA companies who "do that PCI compliance thing"
- No lack of bad information (Search Engines)
- https://goo.gl/MQWQUA - QSA Research Tool

WHERE DOES ONE START?

... FOR THE NEW BUSINESS

GOAL 1 - USE VALIDATED SOLUTIONS

- Utilize validated devices and/or software
  - https://goo.gl/pwAk0I - Pin Transaction Security Devices
  - https://goo.gl/pbRJ8h - Validated Payment Applications
  - https://goo.gl/FWEvpC - Point 2 Point Encryption Solutions
- **Do not “roll your own“ hardware/software**

GOAL 2 - SECURE YOUR ENVIRONMENT

- Utilize latest firewalls, with current subscriptions
- Secure your internal network
  - Patching
  - Anti-Virus, Anti-Malware
  - Use SSL for all data movement
- If you must store Card Data, segmentation is key, encryption is required
  - https://goo.gl/syyqmq - Segmentation Guidance
- Utilize strong authentication (Multi-Factor)
- Strongly consider not using wireless
- Think like a bad guy, "what would happen if?"

GOAL 3 - KNOW YOUR RISKS

- Assess, Evaluate, Manage, Measure
- Know your liabilities (S.B. 601)
- Utilize a third party evaluation (deep knowledge)
- Use this information to create procedures for card handling

COMMON MISTAKES

- “On the Cheap” Purchasing Outdated Equipment
- No insight into Data Trajectory
- Not patching (everything, printers too)
- Bad or incomplete advice from websites/friends/vendors
- Lack of understanding of relevant risks
- Lack of, or poor implementation of, policy frameworks
    - Incident Response Plan

CATCHING UP

… FOR THE ESTABLISHED BUSINESS

SEEK THE HELP OF A QSA

- Conduct a formal CDE Scoping Exercise
- Perform a gap assessment
- Focus on high priorities first (Business Impact Analysis)
  - External Threat(s)
  - Internal Threat(s)
  - Likelihood of Occurrence
- Isolate Card Accepting Systems (Segmentation)
- Eliminate Card Data

FINAL THOUGHTS

- Thoughtful, proactive action is better than hastily concocted solutions
- No one vendor has a monopoly on the "correct answer"
- Well integrated and validated solutions are always better than homegrown

> “Let us not look back in anger or forward in fear,
> but around in awareness.”

–JAMES THURBER

THANK YOU!