connect
Your Independent HP Business Technology Community

NONSTOP
ADVANCED [T.B.C.]

November 3-5, 2013
San Jose Doubletree Hotel
Hosted by Connect and T.U.B.A.

# PCI DSS - A Practical Approach to Compliance

Greg Swedosh
Knightcraft Technology

Knightcraft Technology
Information Security Consultants

NONSTOP
ADVANCED [T.B.C.]

# AGENDA

- Questions
- What is PCI DSS? – A very quick recap
- How to approach PCI DSS
- Traps, Pitfalls and Obstacles
- Other common questions on compliance
- Steps to PCI DSS compliance (checklist)

NONSTOP
ADVANCED [T.B.C.]

# QUESTIONS?

NONSTOP
ADVANCED [T.B.C.]

# QUESTIONS?

Q. When is an organization PCI DSS compliant?

A. When all PCI DSS requirements are in place, as determined by a QSA during a PCI assessment.

Q. Does this necessarily make your cardholder data secure?

A. Not necessarily…. but it is a good start.

Q. Because you are considered compliant today, does it necessarily mean that you will be compliant tomorrow?

A. No

NONSTOP
ADVANCED [T.B.C.]

# QUESTIONS?

## Compliance or Security?

Does your organization approach PCI DSS simply with a view to compliance (a necessary evil), or is it seen as a program to mitigate the risk of credit card fraud?

**As well as striving for compliance, use PCI DSS as an opportunity to improve your security and to "get the house in order" in regards to procedures and documentation.**

# What is PCI DSS? – A very quick recap

- PCI DSS is a data protection standard for payment transaction processing businesses
- Driven by the major card brands, eg AmEx, MasterCard, Visa… with Banks running the validation program
- PCI DSS
  - Baselines the (minimum) controls required to protect, monitor and manage cardholder data
  - Version 3.0 – scheduled for publication November 2013

NONSTOP
ADVANCED [T.B.C.]

# What is PCI DSS? – A very quick recap

- The card brands require PCI status reporting from banks
- The banks require PCI status reporting from merchants
  - Annual PCI assessment by a PCI Qualified Security Assessor (QSA)
  - QSA Report On Compliance (ROC) as per the PCI DSS ROC Reporting Instructions
    https://www.pcisecuritystandards.org/documents/PCI_DSS_2.0_ROC_Reporting_Instructions.pdf

NONSTOP
ADVANCED [T.B.C.]

# What is PCI DSS? – A very quick recap

- The fundamental aim of PCI DSS is to protect cardholder data from being stolen, inappropriately accessed or misused.
- Just as importantly as protecting the data, you need to be able to demonstrate to a QSA that you have taken all of the required measures to achieve the above.
  - Configuration, Documentation, Procedures, Interviews

    (as per PCI DSS ROC Reporting Instructions)

NONSTOP
ADVANCED [T.B.C.]

# What is PCI DSS? – A very quick recap

- Organizations must not only achieve compliance, but must continually maintain compliance – daily, weekly, monthly, yearly… to infinity and beyond.
- PCI DSS is a program, not a certificate!

You don't get one of these!!! →

PCI DSS COMPLIANT

NONSTOP
ADVANCED [T.B.C.]

# How to Approach PCI DSS

# PCI DSS – A Corporate Priority

## Make PCI Compliance a strategic priority

- PCI Compliance is not just about ticking a few boxes and getting a pass. It is about mitigating the risk of credit card fraud.
- Achieving and maintaining PCI compliance must be a directive from senior management within the organization. When conflict arises (which it will), somebody needs to have the power to ensure PCI compliance remains a top priority.
- The card acquirers (i.e. the banks) are now starting to help focus the minds of corporate executives by imposing multi-million dollar fines, if sufficient progress is not being made.

# PCI is a Program not a Project

## PCI Compliance is not a “one off” Project

Initial compliance needs to be set up as a series of defined projects with appropriate budget and resources to do the job,

**BUT…**

there needs to be an ongoing PCI compliance program

- Once compliant, an organization must remain compliant. There is a PCI DSS assessment every year.
- Tools to track compliance from one year to the next make the annual effort easier and more accurate e.g. RSA Archer
  - Each requirement is documented as to how it complied this year, so same documentation, procedures, config can be easily identified and verified next year

# Ensure adequate budget

**Allocate sufficient budget**

You will need appropriate budget for:

- Extra resources. The existing staff probably already have a large workload. You will need more people.
- Extra tools
  - Software to satisfy security/audit requirements
  - Compliance monitoring tools to track progress
- Expertise
  - Provide required PCI training to internal security staff
  - Bring in appropriate expertise to help provide direction. Compliance will be achieved in a quicker and more cost effective way.
  - Liaise closely and continually with your QSA

NONSTOP
ADVANCED [T.B.C.]

# What's the scope?

**Reduce the scope**

In Scope for PCI DSS:

- All system and network components that store, process or transmit cardholder data and any system and network components that connect to these components

So… reducing your scope will reduce your compliance effort

- Do you really need dev systems connected to prod systems via Expand?
- Can you tokenize cardholder data and use those tokens throughout your organization's network?

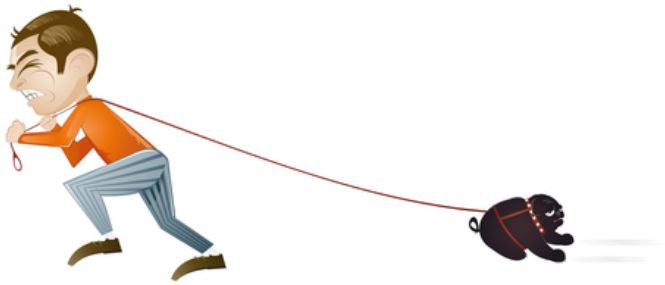
# Traps, Pitfalls and Obstacles

# Competing Priorities

- The Business v PCI DSS
  - PCI can be labeled as top priority, but issues may arise where the business forces PCI to the back seat
    - Delays in upgrade to software
    - Delays in system upgrade
    - Conflict with other planned projects causing delays to PCI project implementation work
  - Senior management must be committed to PCI DSS or it will continually be pushed aside

# Resistance to Change

- Reduction in the use of privileged userids
  - Entrenched use of super.super and application userids on a day to day basis
  - The concept of “least privilege required”
- Changes to access rights
  - The “need” to access and modify critical files without appropriate controls
  - Lack of willingness to embrace change management
- Blame the security
  - The default: If something doesn’t work, blame the new security



# Lack of Resources

- Too much work done by too few
  - Systems managed by very small teams
  - Project scheduled with disregard for how much work systems/application teams already do
  - Lack of continuity as staff dragged off for support or other implementation work
  - Many managers, not enough workers
  - Too many meetings, not enough work
    - With so many people “managing”, too much time can be spent keeping them “up to date”, rather than actually doing the work

NONSTOP
ADVANCED [T.B.C.]

# Overly Focused on Gap Remediation

## Don't just focus on Gap Remediation

- After a PCI DSS assessment, there can be too much focus on simply remediating the gaps that were found.

Q: Will closing all gaps identified in a PCI DSS assessment mean that we are PCI compliant?

A: Not necessarily…

NONSTOP
ADVANCED [T.B.C.]

# Overly Focused on Gap Remediation

## Don’t just focus on Gap Remediation

The PCI Assessment Process:

- For each requirement, the QSA will check the required components e.g. documentation, configuration, procedure.
- As soon as a part of the requirement is determined by the QSA to be “not in place”, the assessment for that requirement will stop.

NONSTOP
ADVANCED [T.B.C.]

# Overly Focused on Gap Remediation

- Don't <u>just</u> focus on gaps…

  Take a holistic approach
- Remember that PCI is a program, not a project
- Remember that the real aim is not simply compliance. It is to mitigate the risk of credit card fraud

# Lack of Separation of Duties

- Security monitoring by system manager
  - Are those with the greatest power and access to the system responsible for monitoring their own access?
- Security managed by application support team
  - Are those with knowledge and access to modify application also responsible for managing security around the application?
- In-house system tools that have been used for years, now questioned as to their acceptability
  - Were they designed, coded, implemented and now used by the same person?

# Lack of Separation of Duties

- Ensure that defined roles and responsibilities exist for all job functions that relate to the NonStop
- Ensure user groups and access privileges correlate with defined roles and responsibilities
  - Identify which roles are performed by each user group
  - Prepare an access matrix detailing which user groups have access to which subvolume types
  - Allocation of subvolumes to subvolume types (file level where required)
- Ensure that there are suitable checks and balances in place to enforce adherence to policy
- Ensure everything is documented

# No clear approach to security

- Who decides who can access what?
  - Is security managed by system manager?
  - Is access provided on request without questioning whether it is really required?
  - Is “trust” used as a mechanism for ensuring that no unauthorized actions are taken?
  - Is anybody ultimately responsible for system security (sys admin? Application manager? Platform owner?)
  - Do security administrators adequately understand NonStop security?

# No clear approach to security

Have a well defined approach to security

- Default access should be NO ACCESS
- A valid reason should be given as to why any access should be opened up
- The reason for access should be analyzed to see if it is truly appropriate and matches with role requirements
- Ensure that role access documentation is kept up to date and is adhered to
- Ensure that there is a specified person with an allocated role who is ultimately responsible for security of the platform

# No clear approach to security

Have a well defined approach to security

- Complete separation must exist between production and dev/test environments
  - Userids/aliases
  - Subvolumes/directories
- Keep it simple and consistent
- Ensure everything is documented

# No clear approach to security

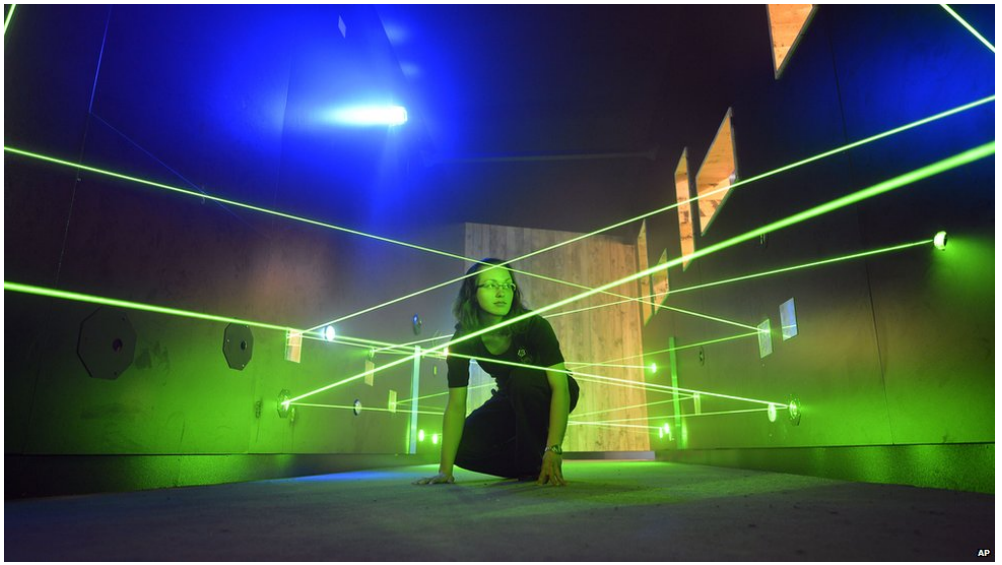
Have a well defined approach to security

- Avoid use of aliases
  - Aliases seem like a useful way of ensuring that privileged user sessions can be tied to an individual
  - But… Guardian and Safeguard have no concept of file security at the alias level (only understand userids)
  - So… user specific files such as TACLCSTM, SCFCSTM, FUPCSTM etc. can be modified by other users
- Avoid using file sharing groups
  - May seem convenient, but provide a lack of security visibility
  - Set security access based on user groups matched with documented roles

# Insufficient monitoring

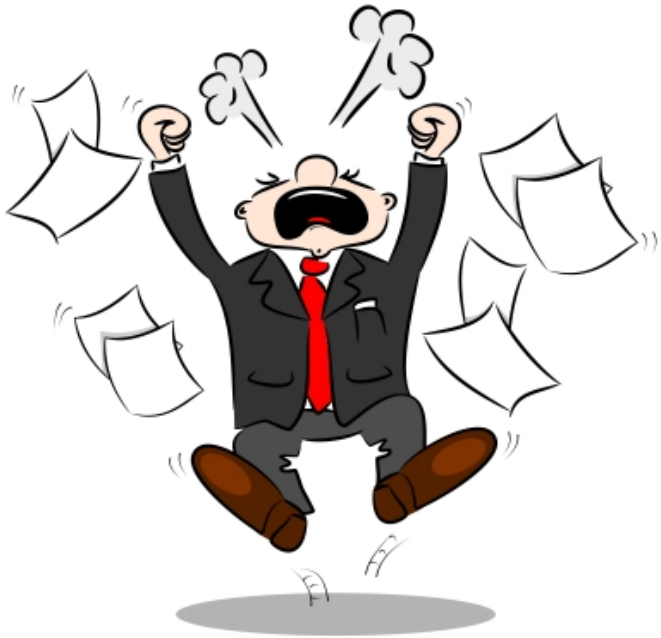
Don’t rely on just one method of monitoring

- A user may be able to hide their tracks from one monitoring method, but it is difficult to hide them if you have multiple methods
  - Safeguard auditing
  - Session capture
  - File Integrity Monitoring
  - Off-box reporting



# DOCUMENTATION!!!

- There's so much… where do I start?
  - The most time consuming work effort required is documentation.
  - Despite knowing it needs to be done and having it up front in the plan, it still gets pushed to the back of the queue.
  - There is no shortcut. Most requirements have a documentation component and it must be satisfied for the requirement to be "In Place".



NONSTOP
ADVANCED [T.B.C.]

# DOCUMENTATION!!!

- Everything needs to be documented
- Begin with Requirement 12
  - "*Maintain a Policy that Addresses Information Security for Employees and Contractors*"
- Take inventory of existing documentation
- Don't leave documentation until last
  - It is a huge job
  - It will be very time consuming

# Security Report Analysis

- Who will read the reports?

  Setting up auditing and session capture is easy, but who will read the reports?

  – If reports and session logs are sent off box, the technical knowledge may not be there to really determine what has happened on the system.

  – If use of privileged userids is excessive, reading through user sessions is an onerous task.

  – This job is boring. Nobody wants to do it.

# Security Report Analysis

Reduce the amount of report data to be analyzed

- Use exception reporting and try to minimize the exceptions!
- All sessions of privileged userids must be analyzed, so minimize the use of privileged userids on the system
- Automate report analysis as much as possible

# Which way to compliance?

## Are we on the right track?

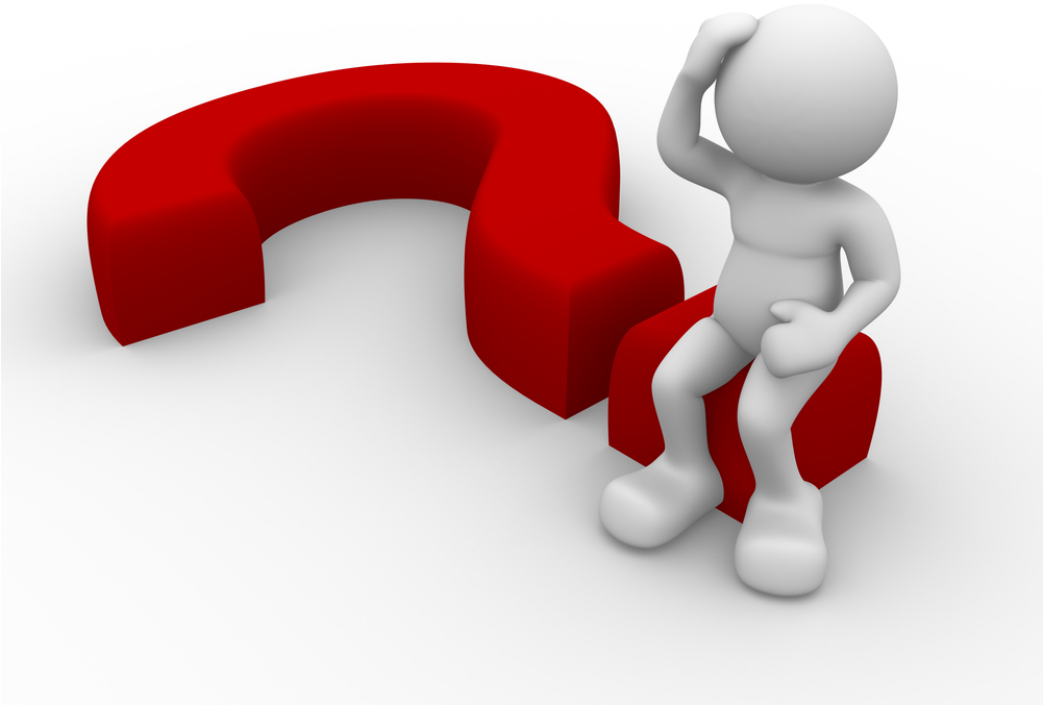
- Are you sure that your planned approach to PCI DSS is the right one?

## Involve your QSA

- Make them part of the decision making process
- They know PCI DSS
- They may have information on how others have approached it

NONSTOP
ADVANCED [T.B.C.]

# Other Common Questions



NONSTOP
ADVANCED [T.B.C.]

# Where is our cardholder data?

- Identify where ALL cardholder data exists
  - Data storage locations
  - Entry and exit points to the application
  - Processes that process cardholder data
  - Networks over which cardholder data is transmitted
- Make diagrams that show the flow of data
  - Payment flow
  - Interfaces to merchants
  - Flow of transactions
  - Network diagram
- Ensure everything is documented

# Where is our cardholder data?

- Cardholder database.
  - Often the PAN (cardholder number) is used as a primary key.
- Transaction logfiles
- TMF auditdumps and audittrails
- Backup media
- Data replication transaction queues (for example those associated with GoldenGate®, DRNet®, Shadowbase® etc.)
- Application trace files
- Communication line/process trace files
- Saveabend (or other memory dump) files

NONSTOP
ADVANCED [T.B.C.]

# Where is our cardholder data?

- Ensure  you know all locations where cardholder data is stored
- No production cardholder data may be used for test or development purposes
- You must demonstrate to the QSA exactly where ALL cardholder data is located and how you determined that this takes in all locations
- Use automated tools to assist you in finding all locations. You may be surprised where it pops up.
- See the article “Where in the world is my credit card data?” in The Connection (April 2013)
  http://www.connect-converge.com/theConnection/TheConnectionApril2013/

NONSTOP
ADVANCED [T.B.C.]

# How do we protect cardholder data?

- Which method to use for PAN data protection as per Req 3.4
  - Encryption
  - Tokenization/Masking
  - Compensating Control providing strong access protection (above & beyond the standard)? [Note that this may only be temporarily acceptible]
- Corporate wide tokenization or encryption strategy?
- Discuss your design/plans for cardholder data protection with your QSA prior to commencing implementation
- Ensure everything is documented

# Does VLE satisfy requirement 3.4?

## Volume Level Encryption (VLE)

PCI DSS Requirement 3.4 states:

*"Render PAN unreadable anywhere it is stored"*

Q. Does VLE on HP NonStop satisfy PCI DSS requirement 3.4?

A. No.

Q. Have some HP customers been adjudged by a QSA to be compliant with requirement 3.4 because they have HP VLE in place?

A. Apparently Yes.

# Does VLE satisfy requirement 3.4?

## Volume Level Encryption (VLE)

PCI DSS Requirement 3.4.1 elaborates:

> *"If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms "*

- Separate authentication does not occur with VLE on the HP NonStop Server.
- The data is not encrypted for ANY user who can access the system (locally, remotely over Expand, FTP etc). You are just relying on file security settings to prevent access.

# Does VLE satisfy requirement 3.4?

## Volume Level Encryption (VLE)

Q: If you rely on VLE to satisfy requirement 3.4 and are considered compliant today, does that mean that you will still be compliant tomorrow?

A: No, not if you get a QSA who fully understands this requirement and the NonStop implementation of VLE.

NONSTOP
ADVANCED [T.B.C.]

# Is BASE24 PCI Compliant?

## BASE24

Q: BASE24 is PCI PA-DSS certified, so does that mean that we will be PCI compliant if we run BASE24?

A: No. There is currently no encryption or tokenization of cardholder data that is provided as part of BASE24.

Q. Why then is BASE24 considered a PCI PA-DSS compliant application?

A. That is indeed a good question.

NONSTOP
ADVANCED [T.B.C.]

# Are we compliant with CONNEX?

## Application Tokenization

Q: We run CONNEX (or other application) with built-in tokenization of cardholder data, does that mean that we automatically satisfy requirement 3.4?

A: Maybe... But not necessarily

This will protect cardholder data stored in the CONNEX database but perhaps data appears "in the clear" (i.e. unprotected) in other locations.

The onus is on YOU to:

- Know all locations where cardholder data is stored
- Make sure that ALL cardholder data is appropriately protected

# Which userids are privileged?

- SUPER.SUPER
- All SUPER group userids
- Security administrator userid (typically the owner of SUPER.SUPER and Safeguard user and protection records)
- Operator userids used for backup and restore
- ISV security software userid
- Application/Data owner userids
- Application builder userids (i.e. userids for implementing new application object code)
- Data replication owner ID
- Any aliases of the above userids

# What should have “deny all” access?

- All operating system files ($system.system, $system.sysnn, DSV subvols, ISV subvols)
- Any files that store cardholder data
- System and OS subsystem startup/shutdown/configuration files
- Security subsystem related files (including third party security software)
- Pathway configuration (no Pathways running with “N” or “A” security!)
- Application files (object code,data, configuration, logfiles etc.)
- Netbatch security including security of all of the job “in files”
- Spooler configuration
- User default subvolume security. These should not be shared and should be secured so that only the owner can create or modify any files.
- Subvolumes on common pmsearchlists
- Process security for $CMON
- Default security for users

# What extra software do I need?

## Standard NSK software

- Safeguard (protection and auditing)
- TACL (TACLLOCL, macros)
- XYGATE Audit PRO (XMA)
- SSL and SSH (comForte)
- XYGATE User Authentication (NB56000 systems)

## What else do I need?

- Protection of data (encryption/tokenization etc)
- PAN detection software
- User session capture
- File Integrity Monitoring
- Other?

# What extra software do I need?

## Vendors

- comForte 21
- CSP
- Greenhouse
- HP
- Integrated Research
- XYPRO Technology

## In-house development?

- Separation between developers and users
- Issues of maintenance and supportability
- Speed of implementation?
- Cost ?

# What extra software do I need?

## Evaluating software

- Make sure that software truly meets your requirements – PCI DSS and internal
- Dedicate time to evaluate fully in your own environment
- Don't just accept vendor claims. Test yourself and try to break it!
- Raise support calls and see how well the support process works
- Some help on what to look for in your evaluation and what questions to ask is provided in the *PCI DSS Compliance for HP NonStop Servers* white paper.

NONSTOP
ADVANCED [T.B.C.]

# Steps to PCI DSS Compliance

- Set ownership of PCI DSS compliance with senior management within the organization
- Approach PCI DSS as an ongoing program, not just a finite project
- Allocate appropriate budget
- Use appropriate tools to track compliance going forward
- Communicate clearly and often to all staff on the importance of PCI compliance
- Educate staff on how changes will affect them in their daily job
- Wherever possible, reduce your scope
- Make documentation a high priority - It is a huge job

NONSTOP
ADVANCED [T.B.C.]

# Steps to PCI DSS Compliance

- Ensure you have appropriate personnel resources
- Identify personnel for critical roles – security ownership, report analysis
- Bring in expertise to help you in your task – QSA, Consultants, Staff Training
- Make realistic schedules for compliance sub-projects - factor in other projects and unexpected delays
- Don’t just focus on compliance. Use a holistic approach to ensure cardholder data is secure and to mitigate the risk of credit card fraud.
- Ensure that you know where all of your cardholder data is located

# Steps to PCI DSS Compliance

- Make sure that you end up with the best software to match your requirements. Evaluate thoroughly and ask the vendors lots of good questions.
- Have a clear and consistent approach to security configuration. Keep it simple.
- Expect the path to be a bit bumpy and prepare accordingly

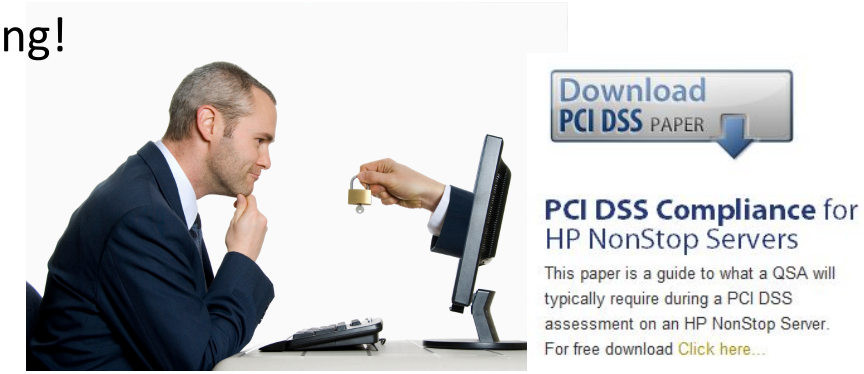
NONSTOP
ADVANCED [T.B.C.]

# Steps to PCI DSS Compliance

## The Definitive Resource

*PCI DSS Compliance for HP NonStop Servers* – Technical white paper

- Details what a QSA will typically look for and what you need to do for EVERY requirement of PCI DSS
- Includes section on evaluating security software to meet your PCI compliance needs
- Steps on preparation and how to approach a PCI DSS assessment
- Information on cardholder data, privileged userids, security config etc.
- Download the latest version for free from www.knightcraft.com
- Version 3.0 is coming!



NONSTOP
ADVANCED [T.B.C.]

# Knightcraft Technology

HP NonStop Security and PCI Compliance Specialists

## PCI DSS Consultancy

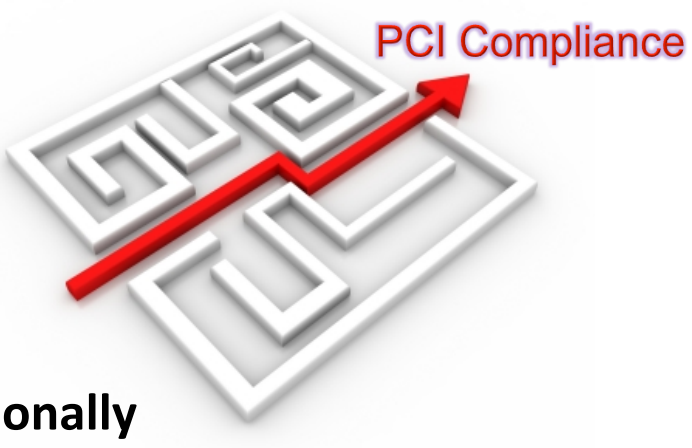
- Help to achieve compliance in a fast, reliable and cost-effective manner. Make sure you're on the right path!

## Security Implementation

- Best practices HP NonStop Security configuration
  - Safeguard, OSS and XYGATE specialists

## Documentation

- PCI DSS documentation. We know what's required.




*** Onsite and remote services available internationally**

Email: greg.swedosh@knightcraft.com
See our website: www.knightcraft.com