Hewlett Packard
Enterprise

Knightcraft Technology
Information Security Specialists

# Are your HPE NonStop systems secure?

## HPE-Knightcraft Security Review

# Contents

# Introduction

Knightcraft Technology
Information Security Specialists

Hewlett Packard Enterprise
Technology Partner
Server Tested
SILVER PARTNER

– HPE NonStop Security and PCI DSS Compliance Specialists.
– Providing professional services to HPE NonStop customers for over 25 years.
  – Australia, New Zealand, UK, USA, Asia, Europe, South America, Middle East
  – Banks and financial institutions, retailers, telcos, governments
– Hands on implementation expertise in HPE NonStop, XYGATE, comForte.
– Partner with QSA to perform PCI DSS assessments.
– Author of *PCI DSS Compliance for HPE NonStop Servers* white paper.
– Co-author of the book *Securing HP NonStop Servers In An Open Systems World*.
– Presenters on security at HPE NonStop Advanced Technical Bootcamp.

**Greg Swedosh, CISSP**
**Senior Consultant**

# The Need For Security

# The Need For Security

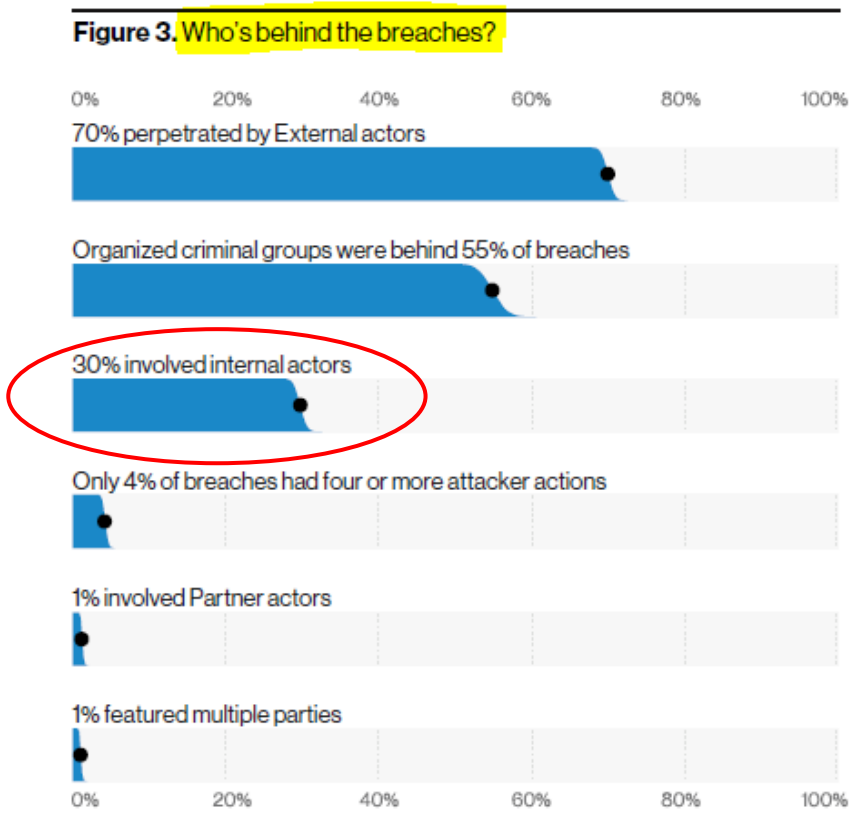
## Data breaches of large corporations are a regular occurrence

- The average total cost of a data breach in 2020 was $3.86million.
- The average cost per lost or stolen record in 2020 was $146.
- Customer PII was the type of data most often lost or stolen in breaches.
- Average time to detect and contain a data breach is 280 days.
- Average cost savings of containing a breach in less than 200 days vs. more than 200 days is $1.12million.

Source:

The Ponemon Institute 2020 Global Cost of a Data Breach Study (https://www.ibm.com/security/digital-assets/cost-data-breach-report )

# The Need For Security




"Keep an eye on employees and periodically monitor their activities. Do not give them permissions they do not need to do their job"

Source: Verizon 2020 Data Breach Investigation Report (https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf)

# The Need For Security

## Changing Regulations and Expectations

The requirement to protect the private information  of citizens is being reflected more and more with the advent of strong regulations and accountability around the protection of data.

- PCI DSS – Payment Card Industry Data Security Standard
- GDPR – Europe's General Data Protection Regulations
- CCPA – California Consumer Privacy Act
- LGPD – Brazil's Lei Geral de Proteção de Dados
- POPI – South Africa's Protection of personal information

# HPE NonStop Server Security

## A secure computing platform **IF** configured appropriately

- HPE NonStop – Inherently a secure platform
  - No shared memory by processes
  - No known viruses
  - Strong security subsystems
    - Included in operating system
    - Add-on products

- **BUT...**
  - the security of any system is only as good as its configuration
  - How can you know if your system is configured in a secure manner?

# The Security Review Process

# The Security Review Process

## Professional expertise to determine exactly how secure are your systems

Security Review

- HPE-Knightcraft Security Review Service
  - Discussions with relevant staff to determine what system access is required for various groups and individuals.
  - Gathering of configurations, documentation and procedural information.
  - Analysis of gathered information.
  - Findings and recommendations written up in a comprehensive report.
  - Summary of findings and recommendations presented to management.
  - Service comprises both onsite and offsite components.
  - An initial review of a customer environment typically takes 3 to 6 weeks of work effort, depending on the specific customer environment.
  - Subsequent reviews are much quicker.

# The Security Review Process

## The Steps

### Kickoff

- Agree the aims of the review.
- Identify specific areas of focus.
- Establish expectations.

### Discussions

- Meet with a sample of people from all depts. Who need access to the systems.
- Identify what their role is and what actions they typically need to perform on the system to do their job.
- Meet with a sample of Information Security Group and relevant management to ensure corporate security objectives are understood.

### Information Gathering

- Collect configuration information from the systems.
- Collect relevant documentation.
- Collect information regarding relevant procedures.

### Analysis/Report

- Analyze collected information.
- Well established methodology.
- Prepare report detailing the findings and recommendations.

### Present Findings

- Deliver report.
- Presentation to management.
- Discussion of findings to ensure that findings and best ways forward are understood.

# The Security Review Process

## Approach

- A collaborative approach.
  - Ensure that staff do not feel threatened. It is not a blame game of who did what wrong.
  - Understanding that security configuration and set up evolves and changes over time.
  - Often the people who initially set things up have moved on and nobody really understands how things are today.
- A pragmatic approach to ensure that staff are able to efficiently perform their required authorized tasks, while not compromising security.

# The Security Review Process

## Information gathering

– Discussions with representative sample of those who access the systems and those responsible for security within the organization.

– The configuration information is gathered by running a series of obey files (scripts) using a non-privileged userid (with the exception of userid information that requires super.super).
  – No special access or remote access to the customer system required.
  – No software needs to be installed on the system.

– Any security related documentation that exists is gathered.
  – Corporate security policy documents.
  – NonStop specific security policy and configuration documents.
  – Startup and shutdown procedures for security related subsystems.

– Any transfer of information via email or similar means is done securely using AES256 encryption.

# The Security Review Process

## Analysis

- Detailed analysis of current security configuration.
- Analysis of security related procedures.
- Analysis of security related documentation.
- Analysis of security event monitoring.
  - Reporting.
  - Alerting.
  - Event delivery to SIEM device.
- Analysis of control and usage of privileged userids and passwords.
  - super.super, super userids, application owner userid, security userid etc.
- Analysis of controls between production and development environments.
- Analysis of typical system areas where privileged userid capabilities can be gained if not configured optimally.

# The Security Review Process

## Analysis

### Areas to review (at a minimum)

- Safeguard configuration.
- Guardian and OSS file and object security.
- ISV security software configuration.
- Userids and aliases.
- Privileged userid usage and management.
- Application object and data access.
- Pathway.
- Netbatch.
- TACL environment.
- SSL/SSH configuration.
- User session and file transfer encryption.
- Kernel managed processes.
- Expand.
- TCP/IP configuration & listens.
- Licensed and Progid programs
- Spooler.
- Reporting.
- Alerting.
- Production and development segregation.
- Web services.
- Patching levels and procedures.
- Documentation

# The Security Review Process

## Deliverables of the HPE-Knightcraft Security Review Service

- Agreed upon statement of work that incorporates the organization's aims and expectations for the review.
- Comprehensive report containing details of all findings with specific recommendations for remediating gaps in security, compliance, procedures and auditing.
  - Identification of configuration vulnerabilities and suggested steps for mitigation.
  - Identification of weaknesses in security related procedures and/or documentation with advice on how these can be improved.
  - Summary section providing a brief outline of the findings and recommendations.
  - Detailed section that explains fully the findings and recommendations.
- Presentation to management summarizing findings and recommendations described in the report.
  - Opportunity to discuss the results of the review and the best approach for moving forward.

# PCI DSS (Payment Card Industry Data Security Standard)

# PCI DSS Compliance

## The banks and PCI DSS

- Many banks are not PCI DSS compliant.
- Because of their unique relationship, the card brands have not forced PCI DSS compliance on the banks and banks are typically not subject to annual PCI assessments by a QSA.

**However…**

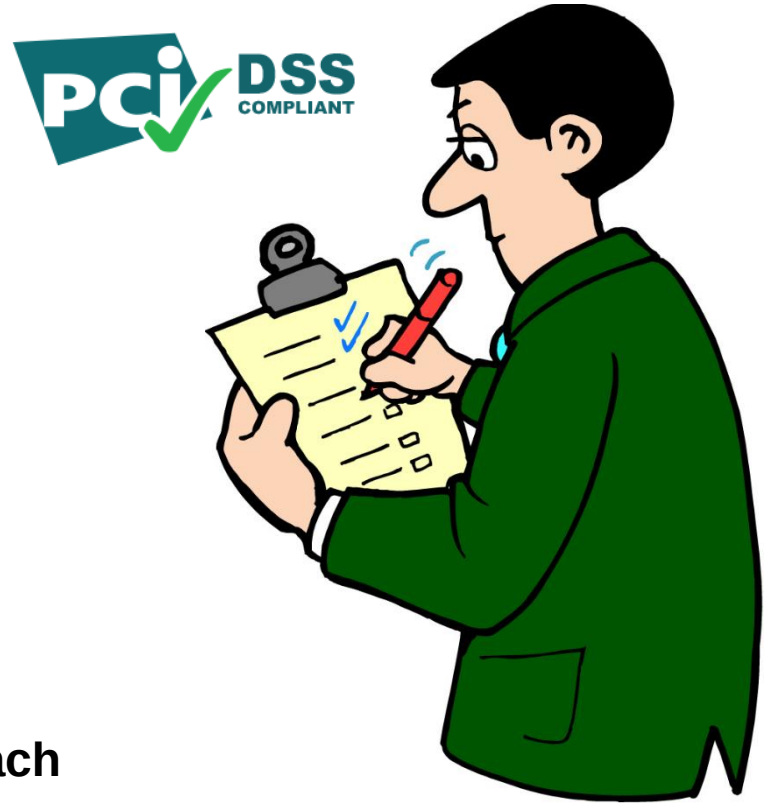
- Banks process and store customer cardholder data, including full track information.
- Protection of this data is critical.
- PCI DSS provides a sound methodology for ensuring your systems and data are secure, whether you be a bank, financial institution, retailer, or in fact any organization that needs to protect sensitive data.

# PCI DSS Compliance

## We are PCI DSS compliant. But are our systems secure?

Many organizations believe that if they are passed by a QSA as compliant with PCI DSS, then that means that their systems are secure.

**This is not the case, as the high profile data breaches tell us!!!**




- TJX Companies 45.6 million cards (2007)
- Hannaford 4.2 million cards (2008)
- Target 40 million cards & 70 million PII records (2013)
- The Home Depot 50 million cards & personal details (2014)

**All thought that they were PCI DSS compliant at time of breach**

# PCI DSS Compliance

## Considerations

- PCI DSS is a strong framework on which to build a secure environment.
- Establishes a multi-layered approach to security.
- Should not be treated just as a tick in the box.
- Just because you have been assessed as compliant, it doesn't mean that your systems are secure.
  - QSAs typically have limited knowledge of the HPE NonStop platform.
  - Checklist approach to compliance.
- Organizations that have experienced a data breach have been shown to not have been truly PCI DSS compliant at the time of the breach.
  - Even if a QSA had assessed them previously as compliant
- Essential to not only achieve compliance, but to maintain it.
  - Security should be reviewed regularly (at least annually).

# PCI DSS Compliance

## PCI DSS Compliance for HPE 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.

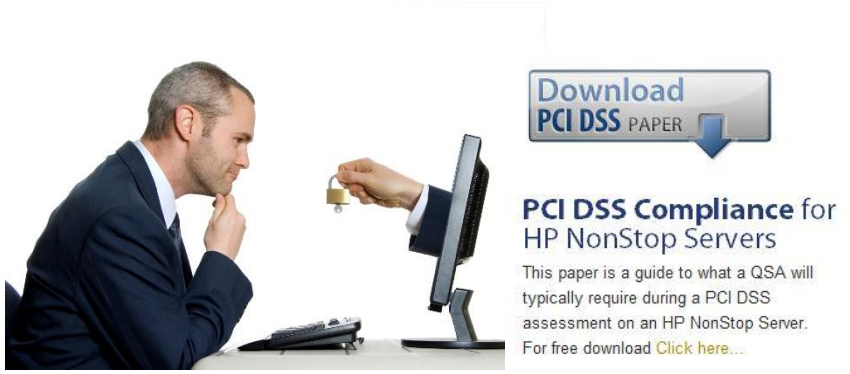
– Independent of any software vendor. Highlights solutions from them all.

– Includes section on evaluating security software to meet your PCI DSS compliance needs.

– Steps on preparation and how to approach a PCI DSS assessment.

– Information on cardholder data locations, privileged userids, security config etc.

– Download the latest version for free from the Knightcraft website




Hewlett Packard Enterprise

# Benefits of an HPE-Knightcraft Security Review Service

# Benefits of the HPE-Knightcraft Security Review Service

- Learn what security gaps exist in your system configurations and how to fix them.
- Learn of weaknesses in your security related procedures and how they can be improved in accordance with industry best practices.
- Identify where your documentation doesn't reflect what is configured on your systems.
- Ensure that your systems are not only PCI DSS compliant, but are also appropriately secured.
- Comply with industry and government regulations.
- Gain the confidence that your HPE NonStop system environment is secure.
- The cost of regular security reviews is extremely low when compared to the extreme cost of a data breach, so it is only prudent for customers to ensure that they truly have a secure environment.

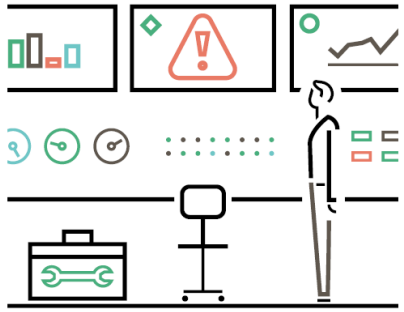
“Cybersecurity teams with a deep-rooted understanding of their businesses will be better placed to anticipate new threats and to recognize potential new aggressors, and to respond ahead of time”

EY Global Information Security Survey 2020
(https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/advisory/ey-global-information-security-survey-2020-single-pages.pdf)

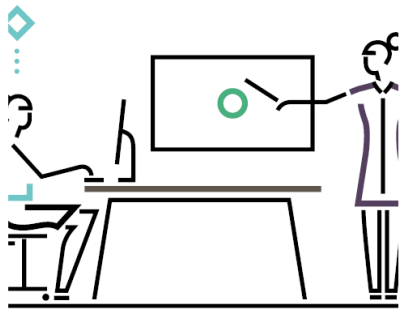
# How HPE-Knightcraft Security Services Can Assist You

Knightcraft Technology in partnership with Hewlett Packard Enterprise

Security Review



Security implementation and configuration



PCI DSS Compliance Assistance

PAN Data Discovery

For more information

- Talk to your HPE account team
- See the Knightcraft website www.knightcraft.com
- Email greg.swedosh@knightcraft.com

*Let Knightcraft Technology, the experts in HPE NonStop server security and PCI DSS compliance, help you to ensure that your systems are truly secure, as well as meeting your compliance requirements.*