Knightcraft Technology
Information Security Specialists

Security?
A never ending story

Greg Swedosh, HPE NonStop Security Specialist

Knightcraft Technology
Information Security Specialists

Chapters

1. Why your security needs a review.
2. Planning your security review.
3. How to review your security.
4. Who should review your security.
5. Getting some help.

Knightcraft Technology
Information Security Specialists

1. Why Your Security Needs A Review

A bit about why this is important

Knightcraft Technology
Information Security Specialists

Why review your security?

Securing systems and sensitive data is more important than ever. Data breaches of large corporations are a regular occurrence and when they occur they are extremely costly.

- The average total cost of a data breach in the USA was $6.5 million in 2015, up 11% on the previous years*.
- The average cost per lost or stolen record was $217*.

*Source: The Ponemon Institute 2015 Global Cost of a Data Breach Study

Knightcraft Technology
Information Security Specialists

Why review your security?

- According to Ernst & Young's Global Information Security Survey 2014*.
  - 38% of vulnerabilities are caused by careless or unaware employees leaving the company exposed.
  - 35% are caused by outdated information security controls or architecture.
- The top threats include attacks seeking to:
  1. Steal financial data
  2. Deface or disrupt their organization
  3. Steal intellectual property or data

* Source: http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf

Knightcraft Technology
Information Security Specialists

We already have PCI DSS assessments. Isn't that enough?

Knightcraft Technology
Information Security Specialists

PCI DSS COMPLIANT

40,000,000

Target had more than this many credit card details stolen (2013).
They thought that they were PCI DSS compliant at the time.
They thought that this meant that they were secure. It didn't.

Knightcraft Technology
Information Security Specialists

Why review your security?

- Compliance does not equal security.
  - Different approach to an audit compared to a genuine security review.
  - Reliance on auditors without sufficient NonStop technical expertise.
- System and application environments change.
  - Upgrades to new systems.
  - New application components.
- Security requirements change.
- Personnel change.
- Technology changes.
  - What was secure yesterday may not still be secure today (SSL3.0 anyone?).

Knightcraft Technology
Information Security Specialists

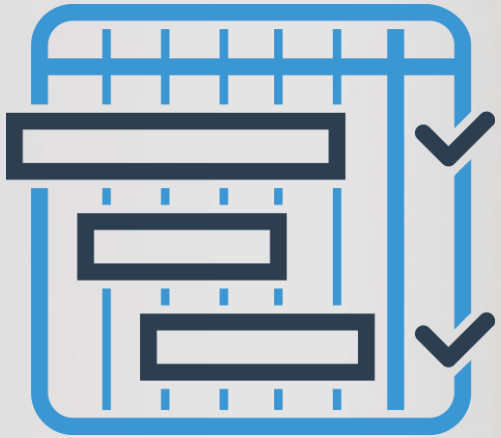
2. Planning Your Security Review

A bit about the approach

Knightcraft Technology
Information Security Specialists

Run the security review as a project

- Create space in your schedule where you can focus only on the review.
- If you try to do other jobs at the same time as the review, it will probably never get completed.
- Allow sufficient time.



Knightcraft Technology
Information Security Specialists

Have an official project launch

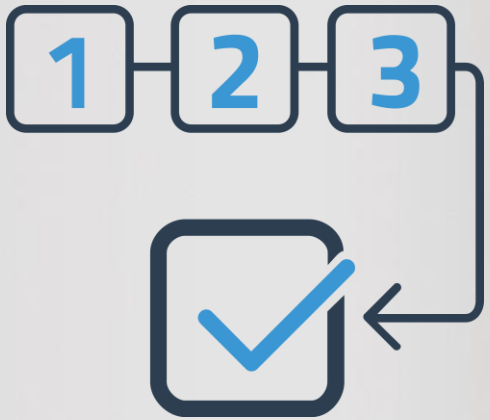
- Set expectations of the review.
- Set a timeframe.
- Set the deliverables.
- Ensure that everybody is on the same page.

Knightcraft Technology
Information Security Specialists

Approach the review in a structured way

- Plan the method of your review.
- Use a structured approach.
- Document everything.
- Where possible, use automation to simplify the process and ensure greater accuracy.

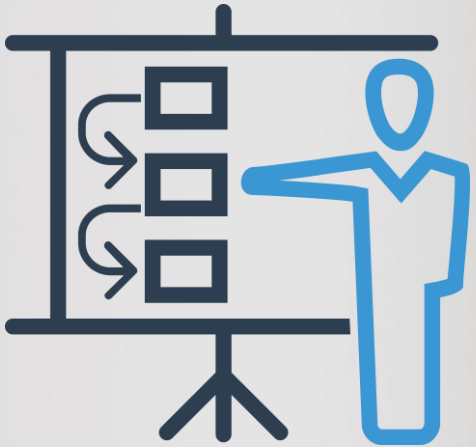
  (Excel is an awesome tool!)



Knightcraft Technology
Information Security Specialists

Present findings to management

- As well as preparing a detailed report, present a summary of the review findings to management.
- Provide suggested next steps for remediating any areas that you feel need addressing.



Knightcraft Technology
Information Security Specialists

3.
How To Review Your Security

A bit about reviewing all that information

Knightcraft Technology
Information Security Specialists

The main aims of a security review

- To identify areas of the system where access is provided but should not be.
  - Sensitive data, privileged information, application objects, system objects.
- To identify areas of the system where privileged userid powers can be obtained in an unauthorized manner.
  - By use of the userid itself.
  - By exploitation of system or application configuration.
- To provide a plan to mitigate any vulnerabilities detected.
- To remove the threat of deliberate or accidental damages.

Knightcraft Technology
Information Security Specialists

The Security Review Process

Project Launch	Interviews	Information Gathering	Analysis	Present Findings
◈ Agree the aims. ◈ Identify specific areas of focus. ◈ Establish expectations.	◈ Meet all stakeholders. ◈ Identify roles and who does what.	◈ Collect the configuration information. ◈ Gather the documents.	◈ Analyze the collected information. ◈ Automate as much as possible.	◈ Write up and present report. ◈ Summary presentation to management.

Knightcraft Technology
Information Security Specialists

Interviews - Who

- Discussions should be held with a representative from all functional groups that access the system or influence security.
  - System managers
  - Operations
  - Application support groups
  - Security administrators
  - Developers
  - Testers
  - DBAs
  - Information security group
  - SIEM administrators
  - Etc.

Knightcraft Technology
Information Security Specialists

Interviews - Approach

- Security reviews can be confronting to staff.
  - Put them at ease.
  - No fingerpointing for any issues found.
  - Evolution of security.
  - Not us vs them.
  - In everybody's interest to get it right. Make it inclusive.
  - Let everybody know what to expect in the review process.

Knightcraft Technology
Information Security Specialists

Interviews - Questions

- For those who access the system.
  - What is their job function?
  - What do they typically do on the system?
  - Which userids/aliases do they typically use?
  - How often do they access the system with privileged userids and typically what for?
  - What procedure is used for gaining privileged userid access?
  - Try and get as much of a sense as you can of what everyone does on the system.
  - Do not assume that you already know the answers.

Knightcraft Technology
Information Security Specialists

Interviews - Questions

- For those who influence or set the security.
  - What aspects of corporate security policy or compliance regulations need to be adhered to?
  - Are there any significant issues that they know of or are concerned by?
  - Try and ascertain their level of NonStop technical expertise.
  - Get a copy of any policy type documentation.
  - If possible, get copies of any previous audit reports.

Knightcraft Technology
Information Security Specialists

Security fundamental principles

- Keep your security model simple and consistent.
  - It will be easier to understand for those who follow you.
  - It will be easier to manage.
- User groups should be set in line with roles & responsibilities.
  - It is better for individuals with multiple roles to have different userids in different user groups i.e. one for each diffent role that they perform.
- Remove the concept of trust from your security paradigm.
- The balance between security and supportability.

Knightcraft Technology
Information Security Specialists

Use of privileged userids

- Are they used on a day to day basis?
- Are privileged userid sessions monitored?
  - Keystroke captured.
  - Sessions reviewed.
- What is the procedure for obtaining passwords?
- Is there a mechanism for ensuring that the sessions are terminated?
- When does the password get changed?
- Are the procedures really really and truly followed?

Knightcraft Technology
Information Security Specialists

Use of privileged userids

- Super.super (Obviously!!)
- All super group userids
- Security administrator userid(s)
- Application/Data owner userids
- Application builder userids
- Data replication owner ID
- Netbatch administrators
- Userids with the ability to modify system/subsystem/application startup or config files or objects.
- Any userids or aliases that have the ability to gain the privileges of any of the above userids using utilities such as XYGATE Access Control (XAC), SECOM, CSP Passport etc.

Knightcraft Technology
Information Security Specialists

Access to data

- Is sensitive data appropriately protected?
  - File security.
  - Encryption/tokenization and associated key management.
- Who has access?
  - In relation to job function.
  - In relation to userids/aliases.
- What access do they have?
- Do they really need access for their job function?

Knightcraft Technology
Information Security Specialists

Areas to review (at a minimum)

- Safeguard global configuration.
- Safeguard, OSS object security.
- ISV security software configuration.
- Userids and aliases.
- Progid and licensed programs.
- Application environment.
- Pathway.
- Netbatch.
- TACL environment.
- SSL/SSH configuration.
- Kernel managed processes.
- Expand.
- TCP/IP configuration & listens.
- Spooler.
- Reporting.
- Alerting.
- Source control.
- Production and development segregation.
- Web services.
- Associated documentation.

Knightcraft Technology
Information Security Specialists

Don’t forget the console!!!

Knightcraft Technology
Information Security Specialists

DON'T IGNORE THE DEVELOPMENT MACHINES!!!

Knightcraft Technology
Information Security Specialists

What all secure systems need (at least)

- Safeguard fully and appropriately configured.
- Minimal and controlled usage of privileged userids.
- Security aspects of all subsystems configured optimally.
- Security events delivered in real time to a SIEM device.
- Encryption of all user sessions (TACL, OSH, FTP etc.).
- Accountability of ALL user sessions.
- Capture of user session keystrokes.
- Integrity monitoring of critical files and subsystem configuration.
- Encryption or tokenization of sensitive data.
- Appropriate reporting and alerting on security events.
- Procedures for ensuring that reports are actually read.

Knightcraft Technology
Information Security Specialists

Resources to assist you

- HPE NonStop Security Hardening Guide***
  (Available from the NonStop Technical Library)
- NonStop subsystem specific manuals
  (Available from the NonStop Technical Library)
- ISV security software manuals
  (Available from your friendly ISV account team)
- *PCI DSS Compliance For HPE NonStop Servers* white paper
  (Free download from http://www.knightcraft.com/pci-dss-3.2)

Knightcraft Technology
Information Security Specialists

4.
Who Should Review Your Security

A bit about whether or not it should be internal personnel

Knightcraft Technology
Information Security Specialists

System managers

Typically have the strongest NonStop technical expertise in the company but…

- Usually already over inundated with work.
- Conflict of interest.
- Usually not security specialists.
  - It’s not just about knowing how Safeguard works.
- A different mindset.

Knightcraft Technology
Information Security Specialists

Security Administrators

Typically have the right mindset and knowledge of general security principles but…

- Often don't have the required level of NonStop technical expertise.
- Also often indundated with other day to day work.
- Perhaps can't see the wood for the trees.
  - Often those charged with implementing security see what they expect to see rather than what is actually there.

Knightcraft Technology
Information Security Specialists

Are your staff already too busy?

- Even if the organization has personnel with the required skills and mindset, they typically have other business as usual type jobs that keep on dragging them away.
- A security review should be a discrete project of known duration. Not an open-ended “do it when I can fit it in” kind of activity.

Knightcraft Technology
Information Security Specialists

5.
Getting some help

A bit about how Knightcraft can assist

How Knightcraft can assist you

Knightcraft Technology
Information Security Specialists

Security Review Service

Security Configuration

PCI DSS Compliance

PAN Data Discovery

Knightcraft Technology
Information Security Specialists

How Knightcraft can assist you

Knightcraft services can be procured from our partners:

Hewlett Packard Enterprise

comForte

For more information:

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

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.

THANKS!

Any questions?
You can find me at
greg.swedosh@knightcraft.com