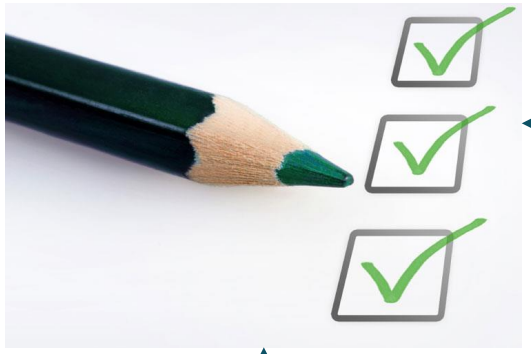
Hewlett Packard Enterprise

4techsoftware™

HELPING TICK THE COMPLIANCE CHECKBOXES WHILE PROVIDING FULL CYBER RESILIENCE

Greg Swedosh
Sean Bicknell

FROM COMPLIANCE TO CYBERSECURITY TO CYBER RESILIENCE



WHAT DRIVES YOUR CYBERSECURITY?

- Industry best practices
- Change in system or application environment
- Change in regulations
- Corporate strategy
- Non-compliance findings
- Failed audit findings
- Security incident
- Management with a big stick
- Other?

WHAT DRIVES YOUR CYBERSECURITY?

https://youtu.be/opRMrEfAIiI

All insider attacks are not malicious

COMPLIANCE

- Compliance is an ongoing requirement
- Standards such as PCI DSS, have good foundations
- Use the standards as a template to build stronger cybersecurity configuration and procedures

SECURITY REVIEW VS COMPLIANCE ASSESSMENT

- Technology changes
- Threats change
- Regulations and standards change
- From box ticking to defense in depth cybersecurity

Compliance Assessment

- Goal: Pass the audit
- Expertise: Low – Usually not a NonStop expert
- Method: “provide as little information as possible”
- Result: Potential false sense of security

Security Review

- Goal: Identify security gaps with view to closing them
- Expertise: High - HPE NonStop specialist
- Method: “On the same side”
- Result: Clear direction of improving security

THE CHANGING CYBERSECURITY LANDSCAPE

- Cyber attacks are becoming more prevalent and more sophisticated
  - Organised crime
  - Nation states
- Not just about data theft
  - Loss or corruption of data
  - Ransomware
  - Disruption of service
  - Illegal monitoring of activities
  - Social engineering
- Insider attacks remain a significant threat
  - Prevalence of remote working

MODERN THREAT DEFENSE STRATEGY – PART 1

Cybersecurity

- Setting up your networks/systems so as to prevent unauthorized access or misuse
  - Policies & Procedures
  - Education
  - Identify your assets
  - Defense in depth – physical, software and configuration
  - Review

IDENTIFY YOUR ASSETS

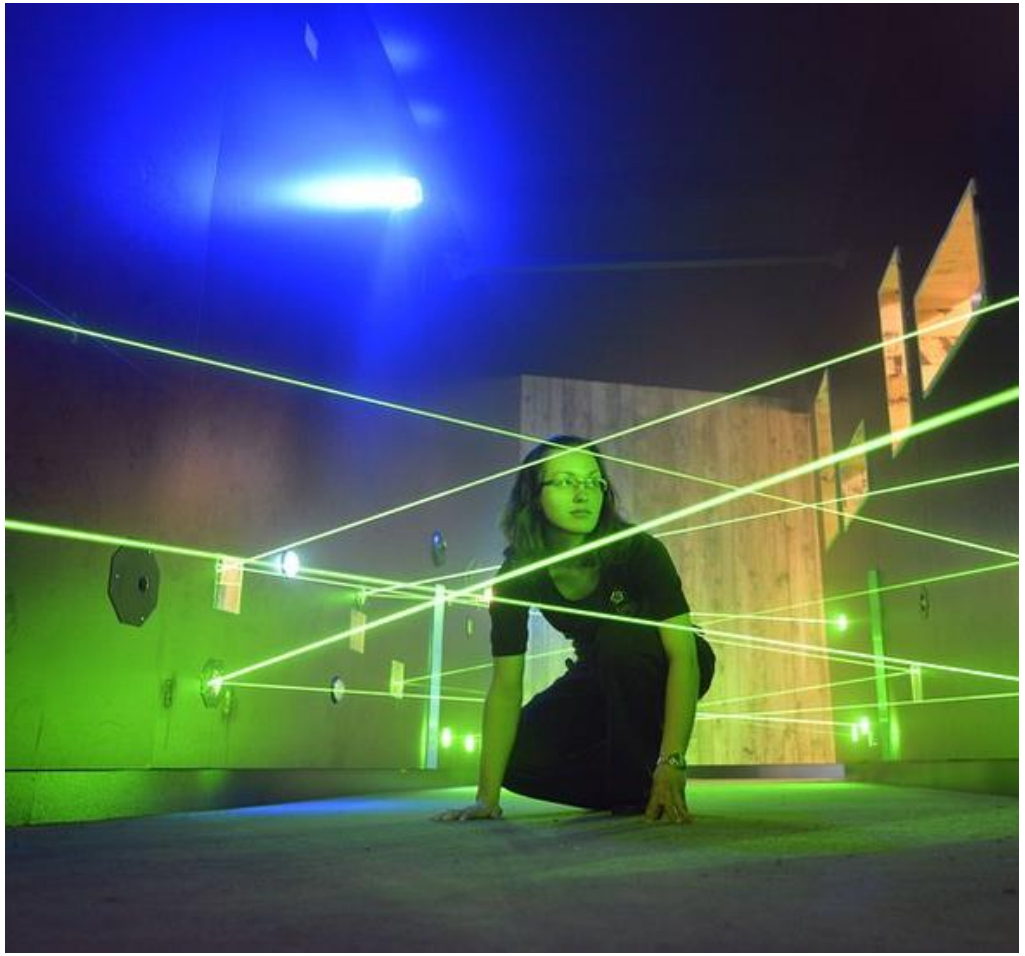
- What are your company's "crown jewels"?
  - Payment card data?
  - PII data?
- Where is it located?
- Do you know all of the places it exists?

To adequately protect your critical or sensitive data, you need to be certain that you know where it exists

DEFENSE IN DEPTH

The Aims:

- To create multiple layers of security controls to protect against different types of cyber attacks.
- To reduce the impact of a cyber attack by slowing its progression through the network.
- To provide redundancy in case one security control fails or is compromised.
- To increase the likelihood of detecting and responding to a cyber attack before it can cause significant damage.
- To protect critical assets and data by implementing security controls that are appropriate for the level of risk.



DEFENSE IN DEPTH

- Strong authentication (MFA)
- Strong access controls to system and data objects
- Strong user passphrases
- Strict control of privileged userids
- Strict security configuration of subsystems
  - Pathway, TACL, TCP/IP, Netbatch
- Monitoring of all user sessions
- Encryption or tokenization of sensitive data
- Data leak prevention
- File integrity monitoring
- Subsystem integrity monitoring
- Session encryption
- “Off box” security logging
- Real time security alerting
- Periodic external review of security

ACHIEVING DEFENSE IN DEPTH ON THE NONSTOP

- You have many of the tools required already, shipped as standard products with the OS:
  - Safeguard
  - NonStop SSH
  - XYGATE User Authentication
  - XYGATE Merged Audit

- The remaining tools required are available from HPE:
  - HPE Tokenator
  - HPE PANfinder
  - HPE Integrity Detective
  - XYGATE Access Control

- Independent Software Vendors also have various security tools that may assist

DEFENSE IN DEPTH

- Strong authentication (MFA) XUA
- Strong access controls to system and data objects Safeguard/OSS
- Strong user passphrases Safeguard
- Strict control of privileged userids Procedures/Safeguard
- Strict security configuration of subsystems
  - Pathway, TACL, TCP/IP, Netbatch
- Monitoring of all user sessions XAC
- Encryption or tokenization of sensitive data HPE Tokenator
- Data leak prevention HPE PANfinder
- File integrity monitoring HPE Integrity Detective
- Subsystem integrity monitoring HPE Integrity Detective
- Session encryption NonStop SSH
- “Off box” security logging XMA
- Real time security alerting SIEM/XMA
- Periodic external review of security

WHAT IF YOUR DEFENSES ARE BREACHED?

Despite your best efforts, it is still possible that your security may be breached.

What then?

THE CHANGING CYBERSECURITY LANDSCAPE

- The cost of Ransomware. To Pay or Not to Pay, that is the question!

Atlanta decided NOT to pay

WHAT IF YOUR DEFENSES ARE BREACHED?

"It couldn't happen on the NonStop!"

Why not?

WHAT IF YOUR DEFENSES ARE BREACHED?

"It couldn't happen on the NonStop!"

Why not?

- Is it technically possible? Yes
- Is there privileged access to the system? Yes
- Does high value data exist on the system? Yes
- Would a down system disrupt our business? Yes
- Could an insider ever be upset enough to maliciously cause us harm? Maybe
- Will your management or security auditors be happy with a response of "it could happen in theory, but we don't think it will, so we're not doing anything"? Unlikely

WHAT IS DORA?

The Digital Operation Resilience Act (DORA)

- An EU regulation that will come into full force on 17 January 2025
- Changes the emphasis from solely ensuring the financial stability of companies to also making sure that they can sustain their operations even when faced with severe operational disruptions caused by cybersecurity and information and communication technology (ICT) problems.
- It seems likely that the UK will invoke similar legislation

MODERN THREAT DEFENSE STRATEGY – PART 2

Cyber Resilience

The ability to resist, respond to, and recover from cyber attacks and disruptions.

- Robust incident response plan
- Isolated recovery system (physical & logical)
- Immutable copies of critical data and files
- Employee training and awareness
- Regular review

CYBER RESILIENCE

- Early detection is key
  - Identification of changes to any critical files
  - Identification of any new program objects appearing on the system
  - Identification of any unknown running processes
- Strong recovery procedures and facilities
  - Regular backups/TMF online dumps
  - Offsite storage (dedicated system, cloud etc.)
  - Isolated recovery system (physical & logical)
- Immutable backups
  - Integrity checking of any files (such as TMF audit dumps) that will be used for recovery.

CYBER RESILIENCE

- Early detection is key HPE Integrity Detective
  - Identification of changes to any critical files
  - Identification of any new program objects appearing on the system
  - Identification of any unknown running processes
- Strong recovery procedures and facilities
  - Regular backups/TMF online dumps
  - Offsite storage (dedicated system, cloud etc.)
  - Isolated recovery system (physical & logical)
- Immutable backups HPE Integrity Detective
  - Integrity checking of any files (such as TMF audit dumps) that will be used for recovery.

FOUR WAYS THAT 4TECH CAN ASSIST

- **HPE Integrity Detective**
  - Early detection of any irregular activity
  - Detect any change to files or subsystem configurations
  - Ensure that your recovery files have not been tampered with (immutable)
- **HPE PANfinder**
  - Locate the crown jewels and ensure that they are only where you think they are
- **HPE Tokenator**
  - Protect your sensitive data by rendering it unreadable to unauthorised access
- **Security review service** (in partnership with Knightcraft Technology)
  - Ensure that your security and recovery implementations are fit for purpose and in line with industry best practices
- All products and services are available from HPE

Hewlett Packard Enterprise

4techsoftware®

Knightcraft Technology
Information Security Consultants

IN CONCLUSION

- Don’t just tick the boxes. Use the standards and your compliance efforts to improve your security
- Implement defense in depth cybersecurity
- Plan for the worst case scenario and be cyber resilient
- Review your security and recovery setup and procedures on a regular basis.
- Talk to your HPE account team about how 4tech products can assist you in achieving your cybersecurity and cyber resilience goals.

THANK YOU

CONTACT:

Sean Bicknell
E-Mail: Sean.Bicknell@4techsoftware.com
WWW: www.4techsoftware.com

Greg Swedosh
E-Mail: Greg.Swedosh@4techsoftware.com
WWW: www.4techsoftware.com