2019 April 02 HPC User Forum Meeting

Cybersecurity and Risk Management and World-wide Standards
Henry Newman CTO Seagate Government Solutions hsn@seagategov.com
Agenda

• Digital Disruption
  • Global Data Explosion
  • Market Transition to Security

• Product Cybersecurity Scope

• Security Certification and Standards

• Manage / Mitigate Risks
  • Compliance and Certification Management
  • Product Security Operations

• Summary
To understand where we are going, it’s important to understand how we got here.
Digital Disruption

1.0 1960 - 1970
Mainframe
Centralized
10 million users

2.0 1980 - 2000
Client-Server
Distributed
2 billion users

3.0 2005 - 2020
Mobile-Cloud
Centralized
7 billion users

4.0 2020 -
Rise of the Edge
Distributed
1+ trillion users

END POINTS
GLOBAL DATA EXPLOSION

The IDC Data Age 2025 report predicts massive volumes of data creation and a convergence of every industry utilizing the value of data.
Market Transition to Security is Occurring

- Majority of data requires at least some form of protection.
- Actual amount of data protection falls far short.
- This gap presents an increasing industry need for security and privacy technologies, systems, and processes to address it.
- Substantial penalties for non-compliance.

Data created in 2025 that should be protected: 90%

Amount that will actually be protected: 45%

- Average Cost of Data Breach in US from IBM and Ponemon study.

GDPR: 2-4% Annual Revenue

7.9M*
Cybersecurity Scope
Lines of Protection

Enterprise Cybersecurity

Integrated Assurance Management

CYBER
PRODUCT
PHYSICAL
DATA PRIVACY / PROTECTION
Cybersecurity Scope
Enabling a Full Lifecycle Data Security Model

Manage Risk
Security Certification and Standards

Authentic Security & Products

Trusted Life-Cycle

Secure Data Disposal

Trusted Data Erasure & Privacy

Security Functionality

Datasphere Protection

Security By-Design

Crypto Module

Trusted Cryptography

Security Algorithms
Security Algorithm Certifications

• Standard and Trusted Security Algorithms

• Certifications of all algorithms
  o Data Encryption
  o Integrity & Signatures
  o Random # Generation
  o Key Derivation…

• Required for FIPS 140-2 & Common Criteria Certs
Security Module Certifications: FIPS 140-2

- Fundamental Security Certification
- Evaluation by Independent Labs
- Required for Information Security Products in Sensitive and Unclassified space in US & Canada
- Value recognized in other geographies
Security Module Certifications: Common Criteria (CC)

• Security Use-Case (Protection Profile) Certification
• Evaluation by Independent Labs
• Certification recognized by 28 member nations globally for Information Security acquisition
Sanitization Standard

- NIST SP 800-88 (Federal) & ISO 27040 (International) define media sanitization
- NIST SP 800-57 Defines Crypto Algorithm Longevity for erasure assurance.
Trusted Life-Cycle Standards

- The Open Trusted Technology Provider Standard (O-TTPS) is now a sanctioned ISO Standard
- Comprehensive Secure Technology Provider Standard
- Sections for Secure Technology Development and Secure Supply Chain
- The NIST Cybersecurity Framework Provides for common framework and language for managing Cyber Risk
Product Cybersecurity Scope
Mitigate Risk

Integrated Assurance Management

- Product Security Operations Center (PSOC)
- Product Security Incident Response Team (PSIRT)

Policy-based compliance aligned to OTTPS, ISO and the NIST Cybersecurity Framework (CSF)

- Identify
- Protect
- Detect
- Respond
- Recover

Policies
- Product Development Policy
- Product Development 3rd Parties

Maturity Staircase to Cybersecurity Compliance
- Gap Analysis
- Conformance
- Certification Preparation
- Certification

Transparent Compliance and Incident Response Management
- Product Security Operations Center (PSOC)
- Product Security Incident Response Team (PSIRT)

Scalable to Trusted Product Lifecycle
- Design, Source, Manufacture, Deliver, Service
Product Security: Manage Risk
Maturity Staircase Based Policy Compliance

- Product Development Policy
- Product Development 3rd Parties

Increasing Levels of Compliance Maturity

- Gap Analysis
- Conformance
- Certification Preparation
- Certification
Product Security: Certification

Trusted Product Life Cycle Certification

ISO 20243
Certify

Identify  Protect
Detect  Respond  Recover

Design
Source
Manufacture
Deliver
Service
# Certified Erase - Strong Data Protection Assurance


### Trusted Tech Provider Standard
- ISO 20243

- Essential & Certified By Design
- Trusted Design & Life-cycle
- Verifiable HW Roots of Trust

### NIST Special Pub 800-88
- Defines Strong Media Sanitization
- Defines Security Requirements
- Defines Erase Certificate. App. D

### NIST Special Pub 800-57
- Defines Security Requirements

### ISO 27040
- Cryptographic Module Validation Program (CMVP)
- Cryptographic Algorithm Validation Program (CAVP)

- Independent Lab Validation
- Validates 800-88 Security Rqmts
- Public Online Policy & Certificate

### Common Criteria for Information Security Evaluation (CC)
- EE – Encryption Engine Profile
- AA – Authorization Acquisition Profile

- Independent Lab Validation
- Validates 800-88 Data Erasure
- Public Online Policy & Certificate
Summary

IP Leakage
Over-privileged Access & Lack of Controls
Confidentiality

Tainted Product
Tampered Product Security Life-Cycle
Integrity

B2B Network Trust
B2B Security Assurance Control / Detection
Availability

Secure Product

Product Security

Managed Risk in Digital Enterprises
Thank You