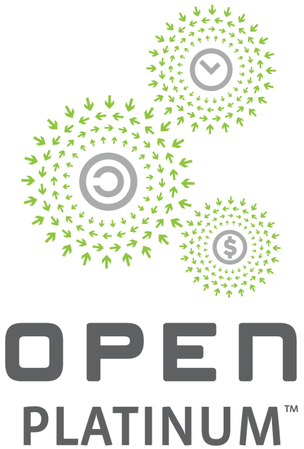

Open. Together.
OCP
SUMMIT

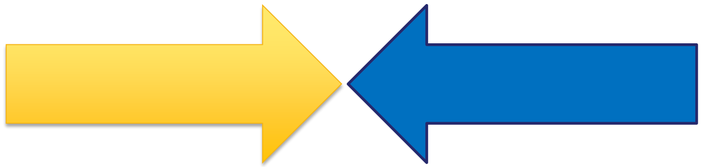
Storage Security from A-to-Z

Arie van der Hoeven, Principal Product Manager
- Cloud Ecosystem Lead, Seagate Technology

Manuel Offenberg
- Managing Technologist, Seagate Technology

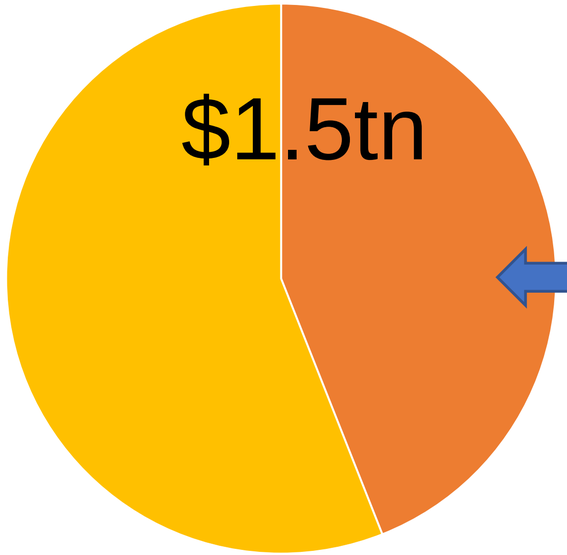


OCP and Device Security - Convergence



OCP Security Charter	Storage Device Security
System boot code integrity	Trusted firmware, known source, audited
Open-source firmware for security hardware	Standards based security practices
Security firmware APIs and protocols	System root-of-trust and attestation
Secure boot of firmware and OS	Secure Boot of storage device
Compromised or untrusted state recovery	Standards based security & policies
Securing/verifying all mutable storage	Firmware is secure and verified with no other mutable storage on the device.
Secure Firmware updates	Secure firmware updates

Data Security Threats



Cyber Crime has soared to a $1.5 + trillion profit business

Data theft represents ~$660Bn +

- Total revenues include:
- $860 billion from illicit online markets,
- **$500 billion from stealing intellectual property or trade secrets "**
- **$160 billion in data trading**
- $1.6 billion in cybercrime as a service
- $1 billion Ransomware

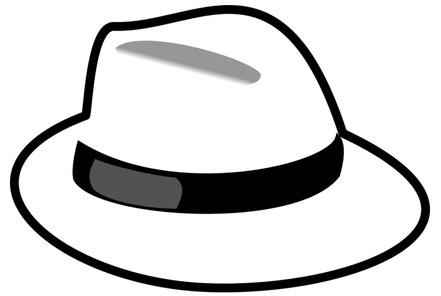
Source: “Into The Web of Profit,” Bromium with criminology researcher Dr. Mike McGuire, University of Surrey, April 2018

SECURITY

Specifications

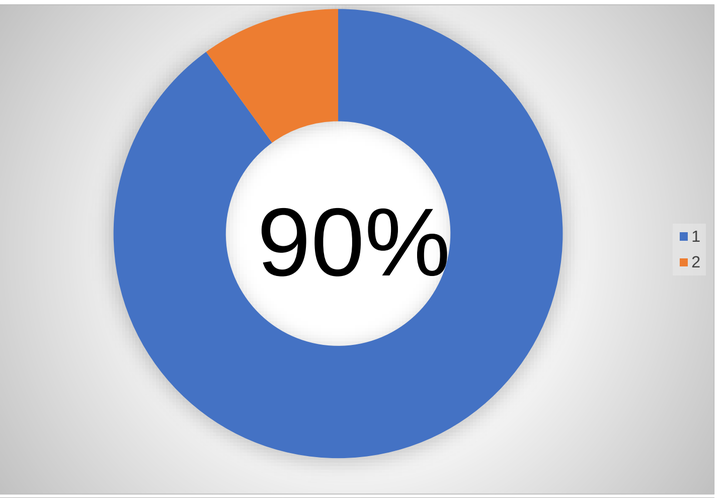
Collaboration and Transparency

- Black Hats work in a highly networked model
  - They buy, sell and share information freely including vulnerabilities and tools
  - Data is increasingly being viewed as the most lucrative target

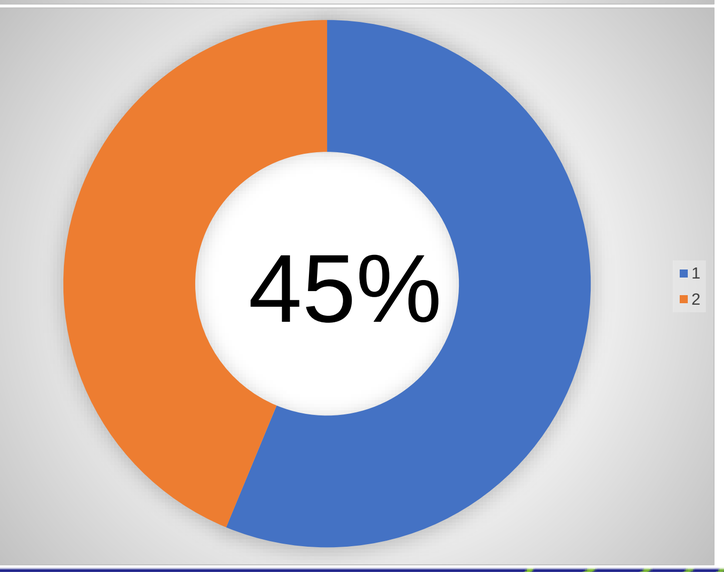


- We must take the same approach
- Assume that hackers know what we know
- OCP is building on existing standards and best practices and led by top tier Security experts who understand this

Transition to data Security



Data created in 2025 should be protected



Amount that will actually be protected

$7.9M per breach*

GDPR: 2-4% Annual Revenue

- Majority of data requires protection
- Amount of data protection falls far short
- Urgent need for technologies, systems, and processes to address
- Penalties for non-compliance
- Standards based
- Motivator for moving to the Cloud if customer requirements can be met

- https://www.pcmag.com/news/362543/how-much-does-a-data-breach-cost
- Average Cost of Data Breach in US from IBM and Ponemon study.

Storage Security Standards

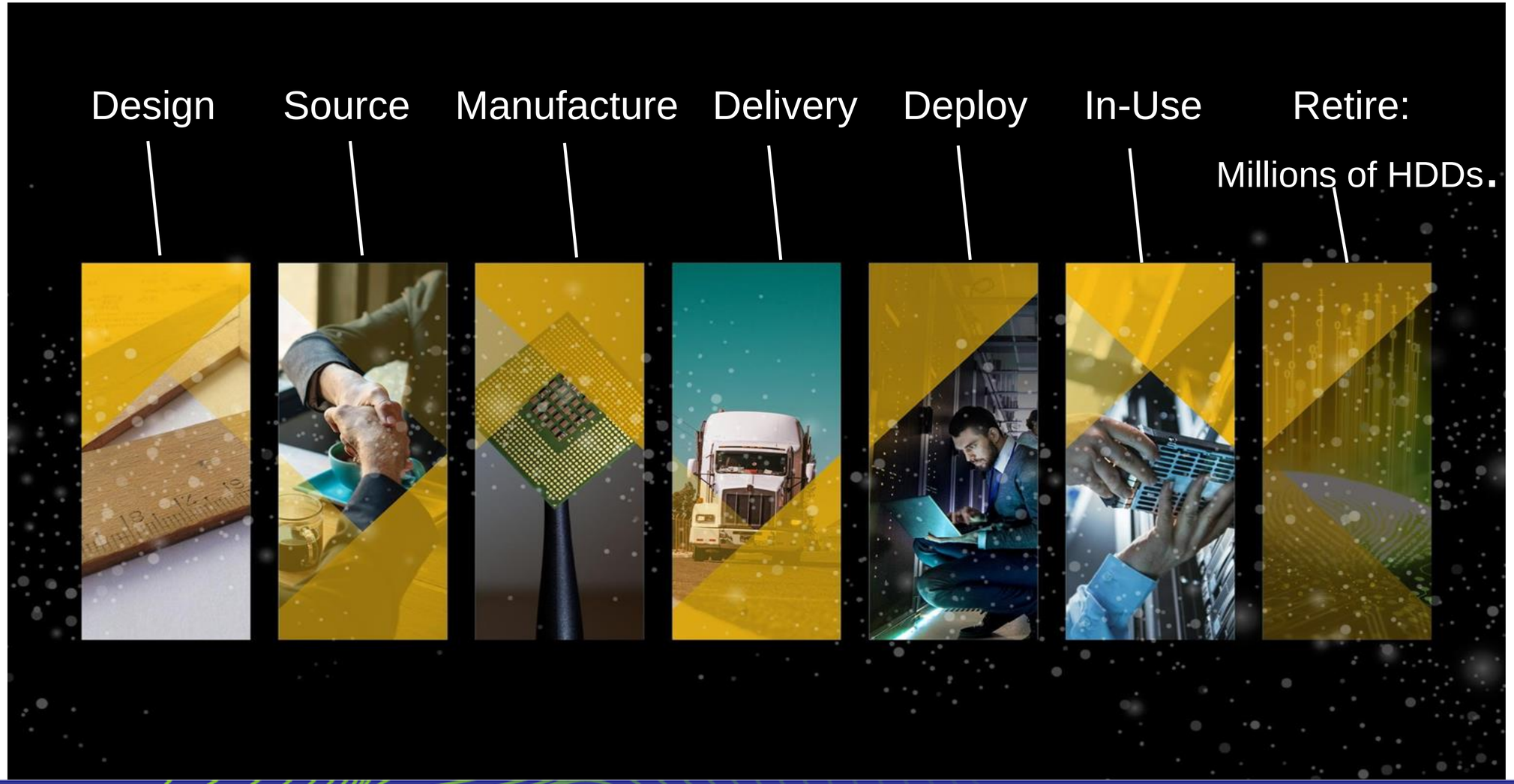
TCG: Trusted Computing Group

- Standards for Secure Storage Protocols
- NIST: National Institute of Standards and Technology

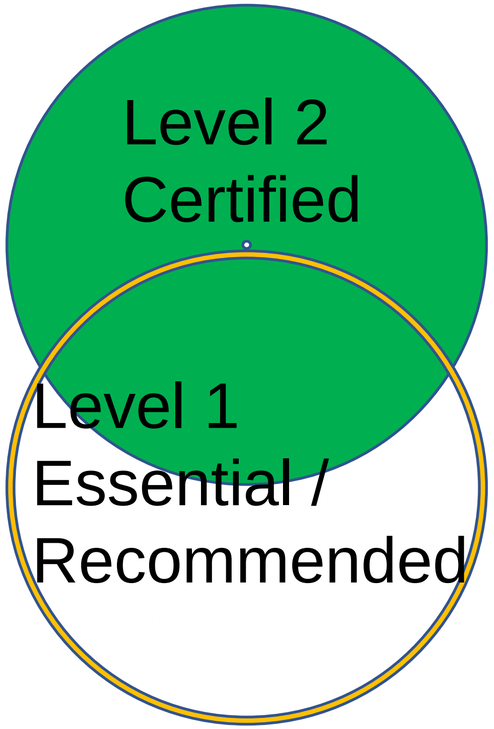
FIPS: Federal Information Processing Standards Certification

- SP: Special Publications
- FIPS 197: AES Encryption
- SP 800-193: Protect, Detect, Recover
- SP 800-88: Media Sanitization
- **ISO: International Organization for Standardization**
- **Common Criteria**
- **Collaborative Protection Profile** (cPP) for full drive encryption (FDE)
- ISO 27040: Storage Security / media sanitization
- **NIAP:** National Information Assurance Partnership

Product and Data Lifecycle Security Model

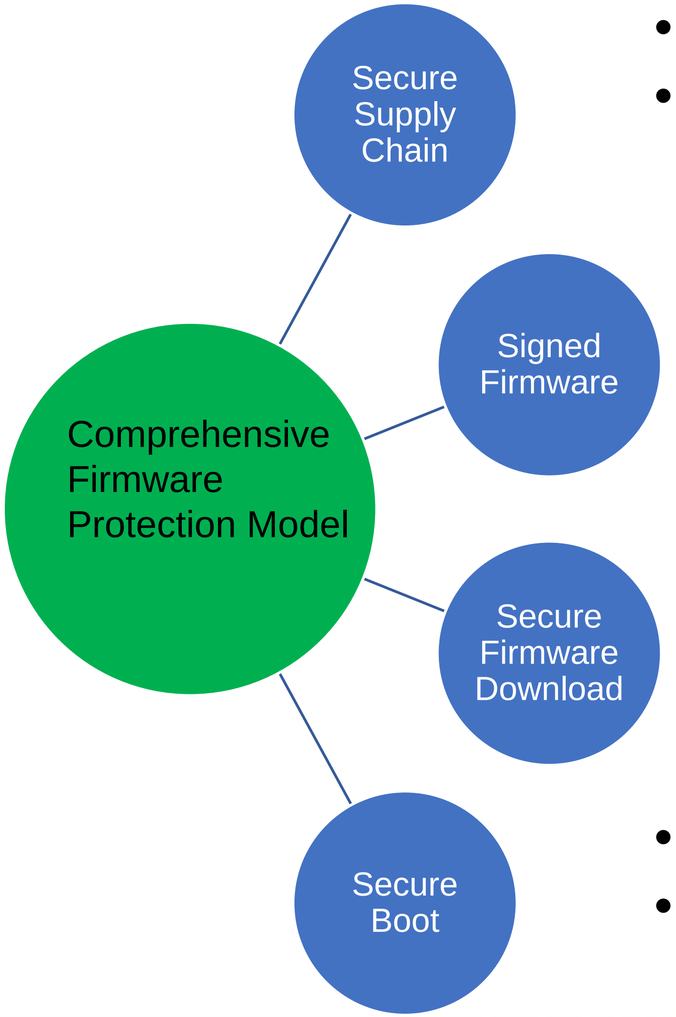


Data Security Solutions



	Essential	Recommended	Certified
Secure Supply Chain	●	↓	↓
Storage Device Root of Trust	●	↓	↓
Secure Download & Diagnostics	●	↓	↓
Storage Device Secure Boot	●	↓	↓
Instant Secure Erase		●	↓
Self-Encrypting Drive		●	↓
FIPS 140-2			●
Common Criteria			●
Trade Agreement Act (TAA)			●

Firmware Protection



- Firmware Protection Begins with Design/Manufacturing
- ISO 20243 Compliance: aka Open Trusted Technology Provider Standard (O-TTPS)

  - Cryptographically Signed Firmware
  - Firmware Rejected if Not Authentic, or Altered

  - Locked Diagnostics Ports Protect Against Unauthorized Users from Downloading/Accessing Firmware
  - Prevents Tampering with FW Executables/System Data

- FW Signature Authenticated by Drive at Drive Startup
- If FW's Encrypted Signature is Modified, Drive Will Not Boot

Why Cryptographic Erase When We Shred Drives?

Cryptographic Erase/Data Protection is Enabled at Power Down of HDD/SSD.

✓ Enables Data Protection from System Removal until Storage Device Arrives at Shredder.

✓ Sanctioned by ISO 27040 and NIST 800-88 – Erasure Meets Clear and Purge Levels.

✓ Added Layer of Protection and Environmentally Friendly Alternative to Shredding.

Certified Erase

- Reduced costs - Many drives can be reused
- Reduced environmental impacts - Drives can be recycled
- Social justice benefits - Reduced pollutant impacts

Trusted Tech Provider Standard
ISO 20243

NIST Special Pub 800-88
NIST Special Pub 800-57

Cryptographic Module Validation Program (CMVP)

Cryptographic Algorithm Validation Program (CAVP)

Common Criteria for Information Security Evaluation (CC)

EE – Encryption Engine Profile

AA – Authorization Acquisition Profile

Call to Action

- Device Manufactures: Participate in the OCP Security Project
  - Send email to OCP-Security@OCP-All.groups.io
- Share customer feedback/perceptions on data security
- Look at the security, cost and environmental benefits of Certified Secure Erase


Open. Together.
OCP Global Summit | March 14–15, 2019
OCP
SUMMIT