HPC User Forum Update

Cybersecurity and Risk Management and World-wide Standards, Santa Fe, New Mexico

Bob Sorensen
May 2019

IN THIS UPDATE

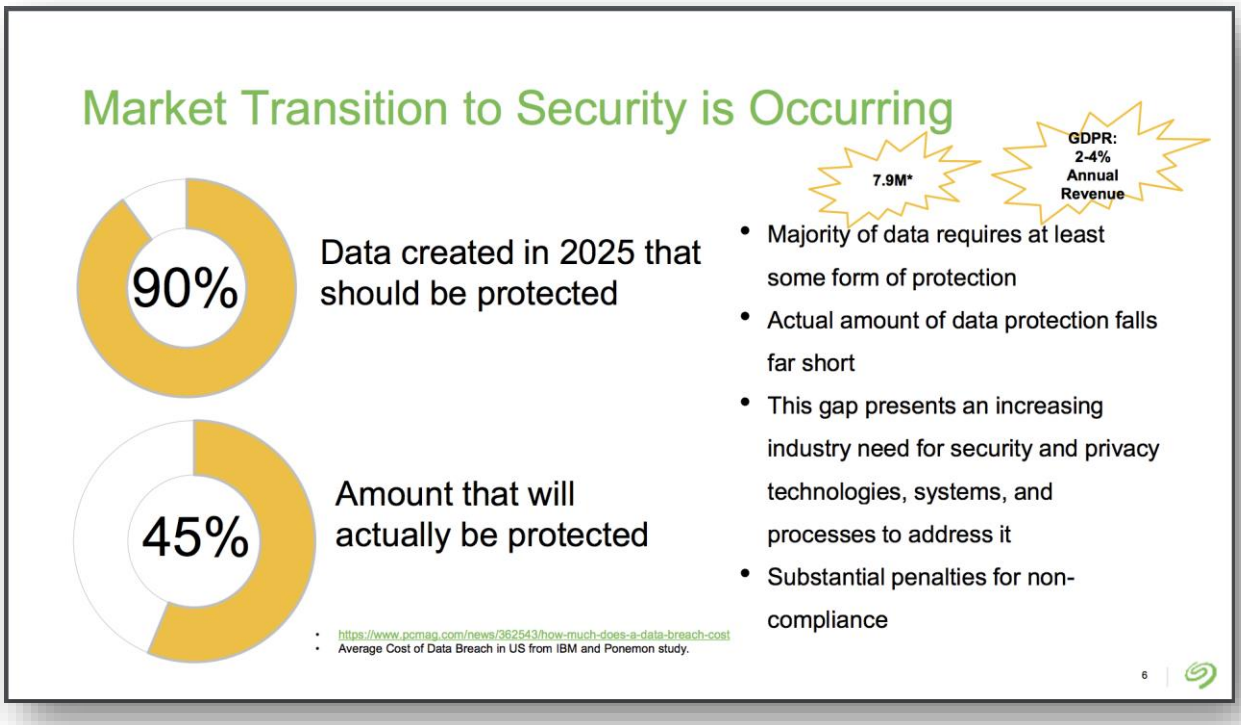
The HPC User Forum was established in 1999 to promote the health of the global HPC industry and address issues of common concern to users. In April 2019, the 72nd HPC User Forum took place in Santa Fe, New Mexico. This update summarizes a presentation from that meeting in the session, entitled *Cybersecurity and Risk Management and World-wide Standards,* given by Henry Newman, CTO, from Seagate Government Solutions.

Source: Seagate and Hyperion Research, 2019

PRESENTATION: CYBERSECURITY AND RISK MANAGEMENT AND WORLD-WIDE STANDARDS, HENRY NEWMAN, CTO, SEAGATE GOVERNMENT SOLUTIONS

Henry Newman from Seagate Government Solutions described the rapid growth of data and the inherent risks involved as the world continues to go mobile. Analysis projects that the world will have 163 zettabytes of data by 2025, with Figure 1 showing the growing gap between data that should be protected and data left unprotected. This gap reflects an increasing industry need for security and privacy technologies, systems, and processes to address it.

FIGURE 1

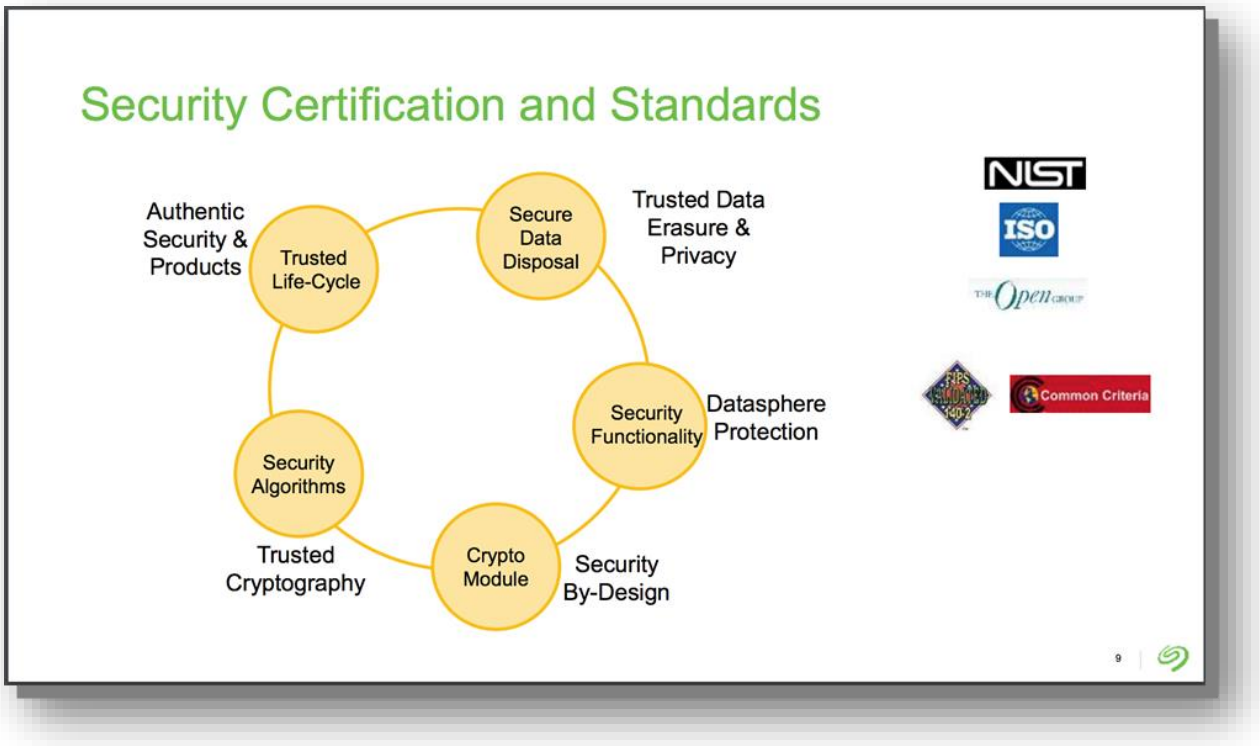


Source: Seagate and Hyperion Research, 2019

Newman described the rising cost of security breaches and potential fines for non-compliance. While these economic forces are driving a market transition to security best practices, the actual amount of data protection falls far short of what is required.

- In terms of password security, Newman noted that ever-growing compute power is already within reach of cracking today's encryption algorithms. The advent of quantum computing in the future could potentially render these authentication technologies obsolete.

FIGURE 2



Source: Seagate and Hyperion Research, 2019

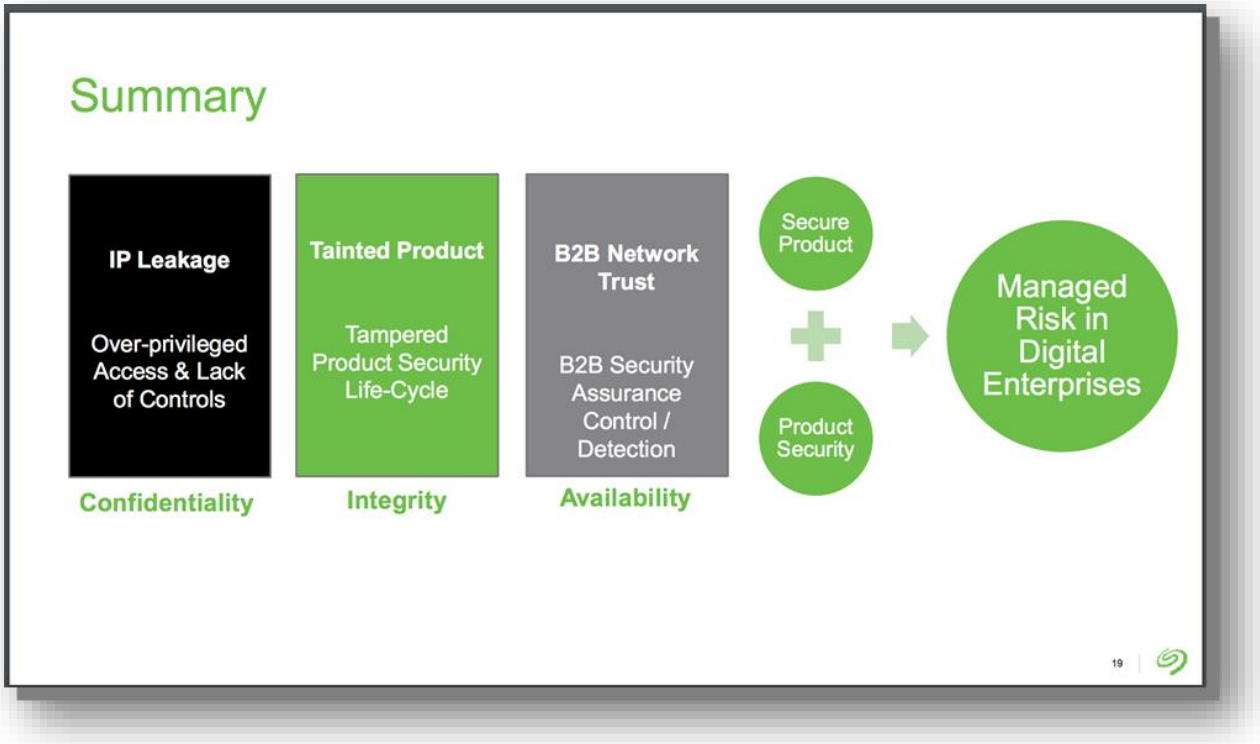
Newman centered the rest of his talk around the data lifecycle and where the data goes.

Newman noted that with exascale capabilities soon to be available in HPC environments, there's going to be more value to data that requires security, so users are going to have more and more problems. Newman cited several security certification and standards to mitigate risk, including Security Algorithms, Trusted Life-Cycle, Crypto Modules, Security Functionality, and Security Data Disposal:

- Security Algorithms (Trusted Cryptography). The two standards come from FIPS and NIST and are required for FIPS 140-2 & Common Criteria Certification.
- Crypto Modules (Security by Design). The Federal Information Processing Standard Publication 140-2 is a U.S. government computer security standard used to approve cryptographic modules. Evaluation is done by Independent Labs and is required for Information Security Products in Sensitive and Unclassified spaces in the US & Canada. The value of Crypto Modules is recognized in other geographies.
- Security Functionality (Datasphere Protection). Common Criteria for Information Security Evaluation (CC) certification is recognized by 28 member nations globally for Information Security acquisition.

- Secure Data Disposal (Trusted Data Erasure & Privacy). NIST SP 800-88 (Federal) & ISO 27040 (International) standards define media sanitization.
  - Secure data disposal is a big problem today because people are reusing drives. Used drives are widely available on the gray market in Asia.
  - Adding to this problem are SSDs, because it is difficult to securely erase them because worn out data cells are no longer addressable with standard SATA or NVMe commands. The data in worn-out NAND cells just gets copied to another cell. For example, in a 1 Terabyte SSD, there are nearly 3 Terabytes of available storage cells in total. Portions of that data can be read but not written-to any more. The only effective way to remove that data is to crypto-erase.
- Trusted Lifecycle (Authentic Security and Products. The Open Trusted Technology Provider Standard (O-TTPS) is now a sanctioned ISO Standard. There is also a Comprehensive Secure Technology Provider Standard and Sections for Secure Technology Development and Secure Supply Chain. The NIST Cybersecurity Framework Provides for common framework and language for managing Cyber Risk

FIGURE 3



Source: Seagate and Hyperion Research, 2019

Conclusions and Issues Going Forward:

- Cyber attacks are an ever-increasing risk.
- There are several existing standards out there for storage and cyber security and more are in the works.
- Following standards is key to combatting future cyber attacks.
- There is a growing threat vector from used drives, counterfeit drives and using devices from the gray market with uncertified firmware.
- Secure erasure is difficult or impossible with SSD drives. Real security requires a custodial approach throughout the device lifecycle.
- There's got to be a stronger level of storage security moving up the stack all the way through the system to follow NIST and ISO standards if users are to protect their ever-increasing stores of data.

For more information or to view this and other presentations given at HPC User Forums dating back to 2008, visit www.hpcuserforum.com.

About Hyperion Research, LLC

Hyperion Research provides data driven research, analysis and recommendations for technologies, applications, and markets in high performance computing and emerging technology areas to help organizations worldwide make effective decisions and seize growth opportunities. Research includes market sizing and forecasting, share tracking, segmentation, technology and related trend analysis, and both user & vendor analysis for multi-user technical server technology used for HPC and HPDA (high performance data analysis). We provide thought leadership and practical guidance for users, vendors and other members of the HPC community by focusing on key market and technology trends across government, industry, commerce, and academia.

Headquarters

365 Summit Avenue
St. Paul, MN 55102
USA
612.812.5798
www.HyperionResearch.com and www.hpcuserforum.com
