Cybersecurity for SSDs

Presented by: Dave Verburg, IBM STSM Storage Technology and Quality

Co-author Samuel Sitorus, Tim Fisher

Agenda

- Data breaches are expensive!
- Supply Chain Security:
  - ISO 20243 vs ISO 27001
- Product Security
  - Secure/Establish trust in the SSD
  - Secure the data at rest
  - Secure the data in flight
- Ransomware detection

Cost of Data Breach

Data Breach (by IBM Security X-Force)

- Business and industries are encountering a growing landscape of cyber security risks.
  - A record high of cost of a data breach in 2022.
  - Extortion was the most common attack impact in most organizations.
  - Phishing was the top initial access vector.
  - Security intrusion was frequently achieved through malwares, mainly backdoor deployment and ransomware attacks

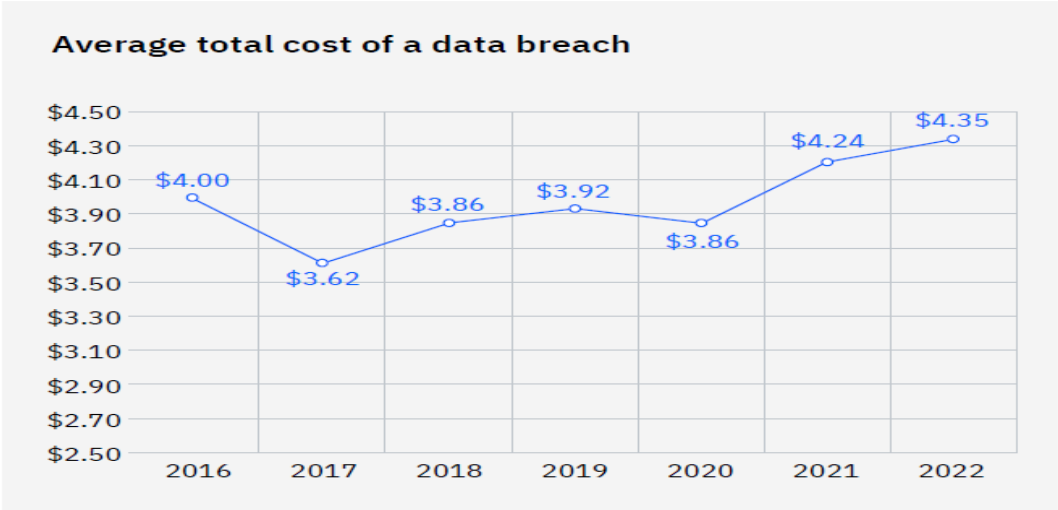

Figure 1: Measured in USD millions

Source : Cost of a Data Breach Report 2022 (IBM Security)

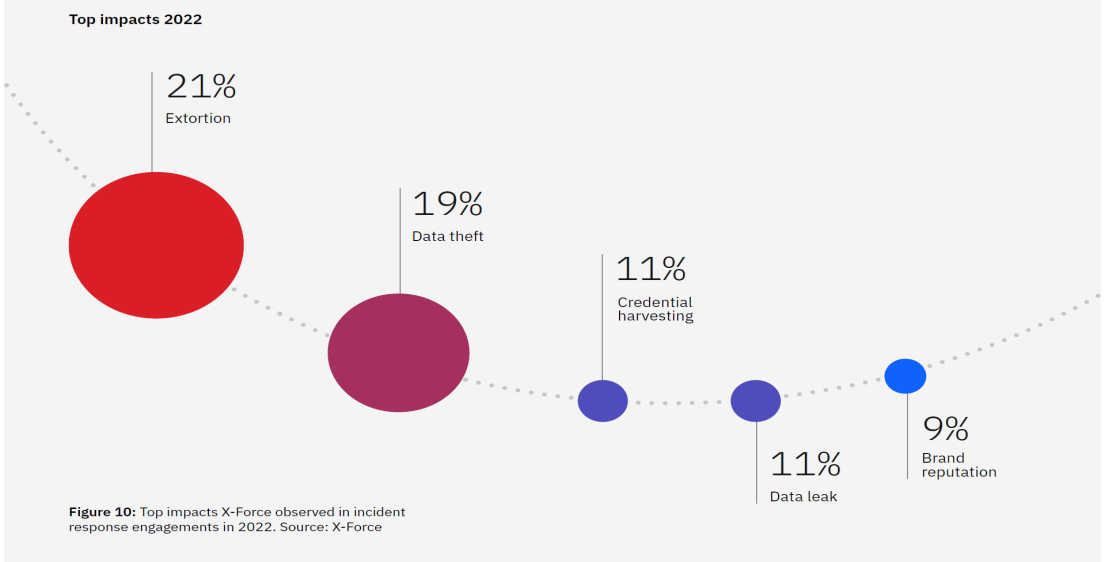

Figure 10: Top impacts X-Force observed in incident response engagements in 2022. Source: X-Force

Source : X-Force Threat Intelligence Index 2023 (IBM Security)

Supply Chain Security

Supply Chain Security

Flash Memory Summit

- “Key material should be protected end-to-end, assuming manufacturing networks are fully compromised.” … Open Compute Project

- ISO 20243 (Published by Open Trusted Technology Provider Standard (O-TTPS, Recommended by IBM)
  - Integrate cybersecurity considerations into the system and product lifecycle
  - Clearly define roles and responsibilities for security aspects
  - Training for key stakeholders in parent org and supplier org
  - Establish protocols for vulnerability disclosure and incident notification
  - Establish requirements for suppliers and assess critical suppliers
  - Know what data is accessible by suppliers/sub-suppliers
  - Explicit roles, structures, processes for supply chain, cybersecurity, product security, and physical security
  - Have visibility into suppliers’ manufacturing processes
  - Mentor/coach suppliers in their cybersecurity practices

- ISO 27001 (Information Security Management System)
  - Security aspects and relationships; Operations, physical, HR, and Information security
  - Incident and asset management and compliance
  - Need to supplement with supply chain security aspects
    - Address specific threats to the integrity of HW/SW products throughout product lifecycle.
    - Visibility to process, not limited to product with flexible scope (IT/OT)

Product Security

Product Security

- Secure/Establish trust in the SSD
  - FIPS
    - Physical security mechanisms to restrict modification/changing module, etc, more stringent with levels
    - Time consuming to get certification
  - Device attestation
    - Verify that a device has access to specific resources; a root of trust (RoT) with the ability to provide evidence of trustworthiness
    - SDPM, DICE, ECDSA, RSA, SHA can be leveraged
  - Secure Boot/Secure firmware download
    - Chain of trust loaded at time of manufacturing; no malicious code
    - RSA, DSA, ECDSA can be leveraged
  - Quantum Safe
    - NIST's post-quantum cryptographic standard expected to be finalized next year
    - CRYSTALS-Kyber (structured lattices) for general encryption selected, four others being evaluated
    - CRYSTALS-Dilithium, FALCON (structured lattices), and SPHINCS+ (hash) for digital signatures
    - With extended product life cycles; Need to be ready to adopt standards quickly

Product Security

- Secure the data (at rest)
  - Encryption
    - SED (TCG Opal/Ruby), FIPS Requirements
    - Access control with keys, encrypted data
  - NVMe Sanitize
    - Sustainability: Need to build trust with the industry so customers willing to return failed drives
  - Configurable NS locking
    - Isolates resources to minimize scope of exposures
  - Key per I/O
    - Provides finer granularity of data encryption; may allow for cleaner erasure strategies
    - Important for multi-user cloud environments; may be more important as CXL enables larger data pools
- Secure the data (in flight)
  - PCIe Link Encrypt
    - With new Cloud, AI, and Analytics usage models, every component can be an attack vector*
    - PCIe-IDE, CMA, DOE, VDM +AES can be used
  - Trust Domain Extensions (TDX) I/O
    - Enables a device to be securely assigned so link data is protected against attacks

* ChipEstimate.com Blog 2021

Ransomware Protection

Ransomware detection

- "Zero-trust" approach
  - Need to be aware and monitoring for attack vectors
    - A computer system needs to work as a unit to monitor
    - Storage devices can monitor for unusual activity and provide hints to a system
    - As an industry we can provide value by fighting cybercrime
  - IBM DS8000 Safeguarded Copy
    - Preserved copies -- granularity, isolation, and immutability
  - IBM FlashSystems Cyber Resilience Solutions
    - Data protection and high availability features with IBM Flash Core Modules
    - IBM Storage Virtualize data management – Storage Protect, Storage Protect for Cloud, Storage Sentinel
  - IBM Storage Defender
    - A unified data resilience for enterprise data storage.
    - Advanced and proactive threat protection with surgical recovery, flexible consumption model, seamless function with modern IT environment, compliance without compromise.

Ransomware Detection

- Example of FCM will use Computational Storage NVMe concepts to provide data collected inside the SSD to a higher-level software stack in our FlashSystem appliances
  - Points to be added this week

Summary

- Costly impact of data breaches across all business and industries.
  - Heightened awareness to take immediate action to address cybersecurity threats
- Supply Chain Security is important.
  - Multi faceted approach is required to manage and mitigate the risk with continuous best practices adoption.
  - Recommend ISO 20243 OTTPS certification to establish holistic security assessment
- Product Security is one of key building blocks.
  - Multi dimensional data protection algorithm/features/techniques to mitigate constantly moving and challenging security risks.
- Cyber-resiliency strategy with “zero-trust” approach.
  - Build “application-aware” solution to enable business acceleration to adapt and tackle known and unknown crises, threats, adversities, and challenges
  - Work as an industry to fight cybercrime

When you interact with IBM, this serves as your authorization to Flash Memory Summit or its vendor to provide your contact information to IBM in order for IBM to follow up on your interaction.

IBM's use of your contact information is governed by the IBM Privacy Policy.