HITACHI
Inspire the Next

The Changing ***Standard of Care*** for Storage

September 22, 2016

Eric A. Hibbard, CISSP, CISA, CCSP
HDS CTO Security & Privacy

Sustain the next era.

Standard of Care???

HITACHI
Inspire the Next

- **Care** – Level of active concern, or lack of negligence, towards avoidance of possible dangers, mistakes, pitfalls, and risks, demanded of a party as a duty or legal obligation. See also due care and duty of care.
- **Due care (Duty of care)** – Degree of care that an ordinary and reasonable person would normally exercise, over his or her own property or under circumstances like those at issue. The concept of due care is used as a test of liability for negligence.
- **Due diligence** – Measure of prudence, responsibility, and diligence that is expected from, and ordinarily exercised by, a reasonable and prudent person under the circumstances.

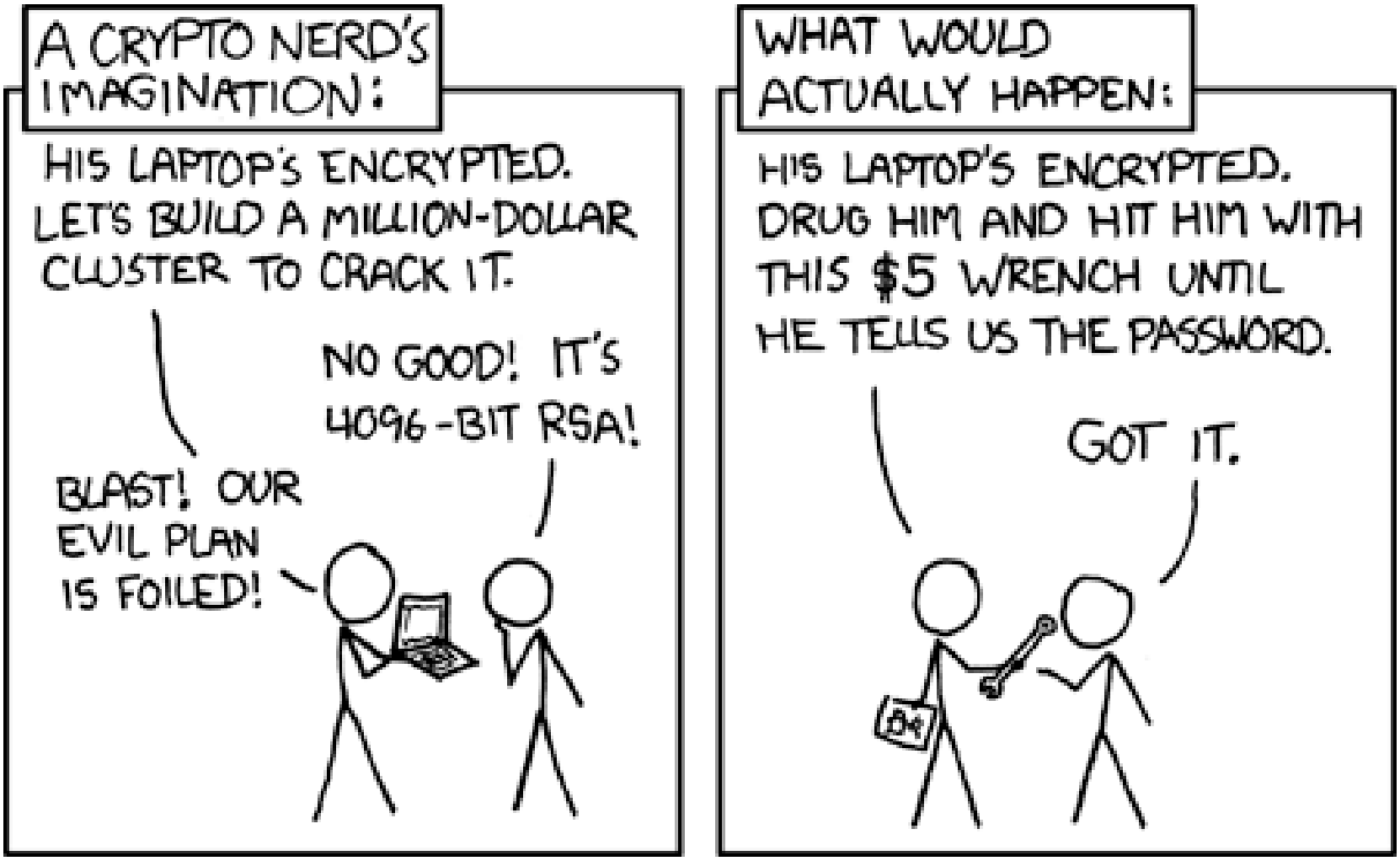
- **Standard of Care** – Degree of prudence and caution required of an individual who is under a duty of care.

Snapshot of Threat Landscape

HITACHI
Inspire the Next

- Drive-by Downloads
- Worms/Trojans
- Code Injection
- Exploit Kits
- Botnets
- Physical Damage/ Theft/Fraud (Mobile)
- Identity Theft/Fraud
- Denial of Service
- Phishing
- Spam
- Rougeware/ Ransomware/ Scareware
- Data Breaches
- Information Leakage
- Targeted Attacks (APT)
- Watering Hole

Humans are the Weak Link



There are countless ways to exploit human weakness, which are infinitely more powerful than “cracking” the security.

Challenges for Storage Practitioners

HITACHI
Inspire the Next

- Many organizations face complying with a wide range of regulatory, statutory, and other legal requirements.
- Storage managers and administrators may be asked to:
  - assist in supporting a variety of legal actions
  - take abstract legal requirements and translate them into implementable solutions
  - help their organizations guard against data transgressions having legal consequences
- Storage implementations can be challenging and necessitate the use of technologies and approaches that are unfamiliar to storage practitioners

Sampling the Requirements

Privacy (Data Protection)

HITACHI
Inspire the Next

- Many countries—the U.S. being a notable exception—consider privacy to be a fundamental human right
- Privacy protection laws have been introduced in a significant number of countries
- The types of “protected” data can vary significantly
- Privacy violations can include the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data

- Redefining the concept of a data breach

Accountability & Responsibility

HITACHI
Inspire the Next

- Increasingly, government officials and corporate executives are being held personally accountable for their actions or lack of action
- Inappropriate data handling or malicious attacks on data can cause individuals and organizations to incur liabilities (civil litigation)
- Unauthorized possession or access of regulated data can result in penalties and force “costly” breach notifications
- Adherence (or lack thereof) to organizational policy can be an important factor in determining negligence

Traceability

HITACHI
Inspire the Next

- Special emphasis on controlling and monitoring privileged users (administrators)
- Data provenance and chain of custody
- Proof of Service (e.g., encryption and sanitization)
- Digital Evidence

Confidentiality

HITACHI
Inspire the Next

- More types of data have to be protected against unauthorized access and exposure
- Protections needed for both data in-motion and at-rest
- Retention periods can be lengthy (crypto agility becomes a concern)

Looking Forward

Changing Technology Space

HITACHI
Inspire the Next

- Cloud Computing
  - Changing consumption models
  - Loss of control of the infrastructure
- Big Data & Analytics
  - Aggregating massive amounts of data (juicy targets)
  - Access controls are often loosened
- Internet of Things (IoT)
  - Massive increase in number of “things” creating data
  - Volume of data expected to increase exponentially

A Few Things to Dread…

HITACHI
Inspire the Next

- Mobile malware will further complicate the threat landscape
- More malware will fill the supply chain. Expect more malicious code in BIOS and firmware updates
- More crimeware will destroy the operating systems (OSs) of targeted systems as a last step of an attack
- The “Internet of Things” becomes the “Internet of Vulnerabilities”
- Attackers will increasingly lure executives and compromise organizations via professional social networks
- Cybercrime gets personal

Looking Further into the Future…

HITACHI
Inspire the Next

- Threat landscape is significantly affected by low frequency large impact events (black swans) as they represent high impact unexpected events
- Privacy is a global issue; expect significant developments with the new EU Data Protection rules
- Advanced persistent threats (APT) are expected to become more common place as existing vulnerabilities are addressed
- Digital currency could open entirely new avenues for attackers
- Many nations are contemplating their cyber warfare strategies and capabilities; some of this is likely to escape into the hands of attackers

Thank You