

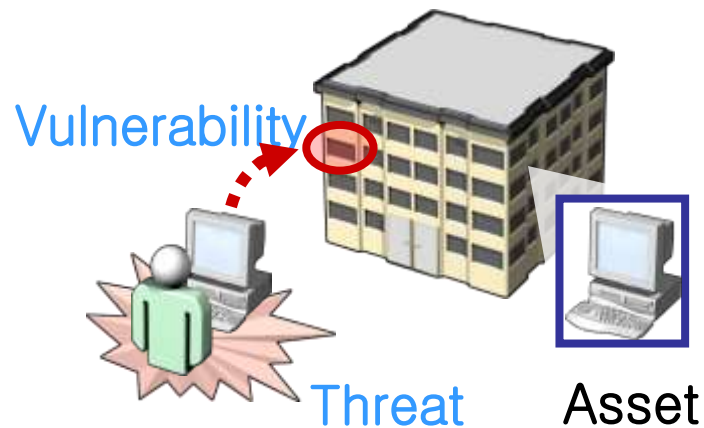
Seven Steps to Delivering a Secure USB Drives Strategy and Policy!

Brian Hawes

Sr Account Rep - Americas

Enterprise Division

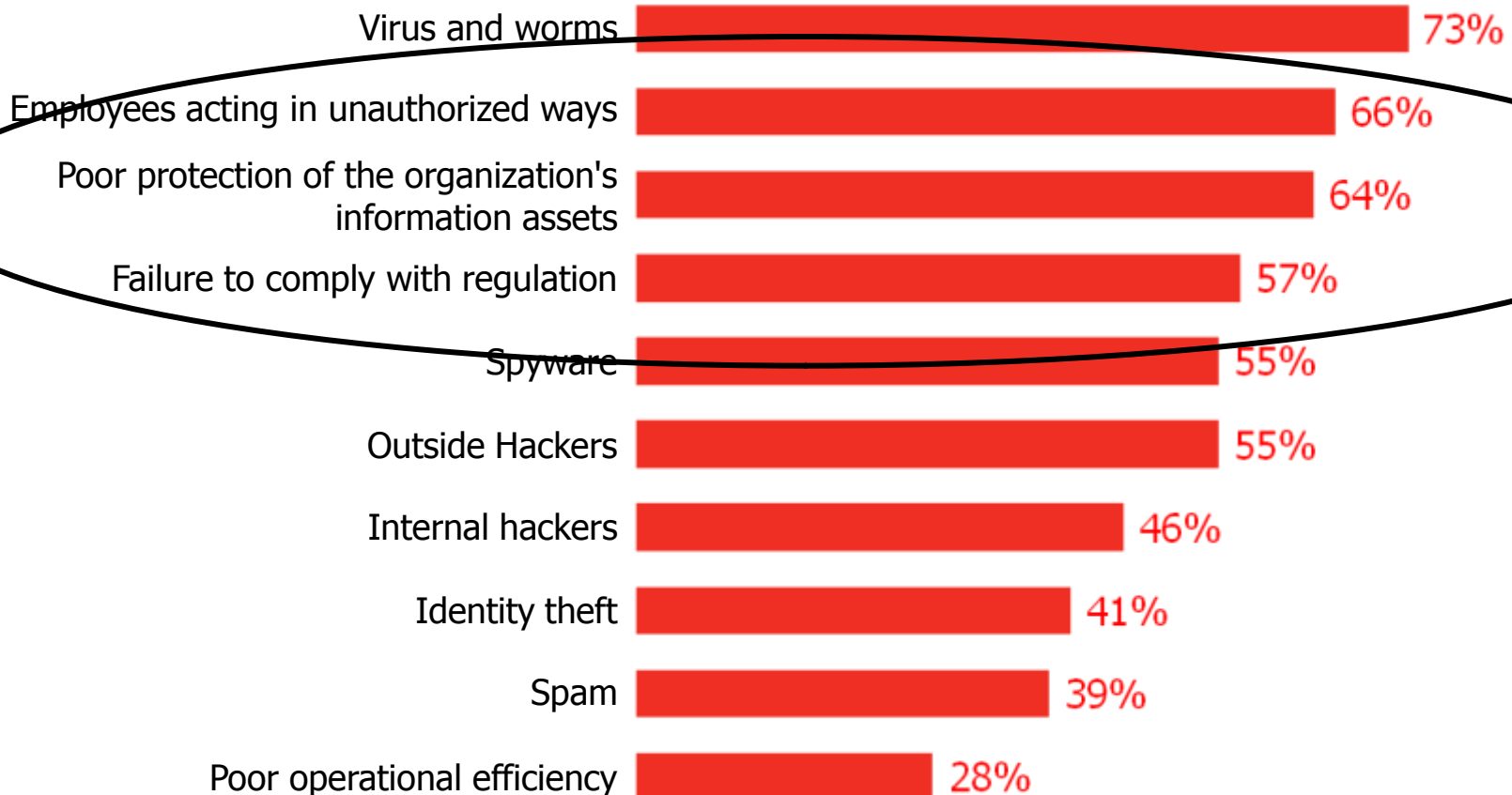
Understanding The Threat



- Information theft and proprietary data leakage are making headlines daily.
- 80% of data theft and misuse is attributed to insiders. The main threat is inside.
- While enterprise networks are typically protected by a variety of security applications, endpoints are often left exposed to threats from within.

Top Enterprise Security Concerns

Percentage of companies that are concerned about the following risks



Source: February 23, 2006, Trends "Fear Factor: Information Assets And Viruses And Worms Top IT Security Threat List"

Base: 149 technology decision-makers at North American SMBs and enterprises.

USB Drive Storage Options



Basic Drives / \$7



Slim Designs / \$44



Titanium coated / \$30-\$90



Ultra Small Drives



Custom Designed Drives
\$\$ Varies

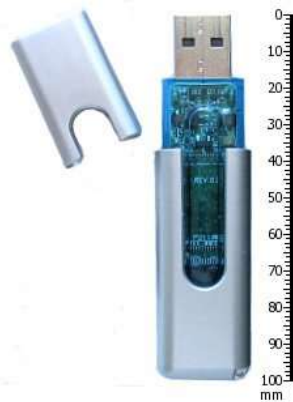


Both Public and Encrypted
Partitions
\$65 - \$300



100% Encrypted Drives / \$75 - \$300

But they Can Also Look Like This...



Security Implications

When an organization's information is stored on non secure and personally owned devices, employees put their employer at risk every time they step out the Door.

Once company data falls into the wrong hands the possibility of threats becomes infinite.

Risks can be classified as follows:

- Data exposure due to device loss or theft
- Unauthorized data extraction
- Introduction of malicious code

Enterprise Concerns

- With millions of USB storage devices in the marketplace, confidential company data is constantly on the move, and simultaneously at risk to loss or theft.
- There is a need for proper security measures that cover these mobile storage devices
- There is a need to maintain user productivity

Dealing With Some Of The Major Concerns

Data Leakage

- Limit the use of USB drives to company-authorized devices
- Manage how they can be used
- Support and manage password access
- Back-up data if required
- Be able to shred data or drive if necessary
- Force encryption at all points

Dealing With Some Of The Major Concerns

Regulatory Compliance

- Identify which compliance requirements apply to your organization... SOX, HIPAA, GLBA, Bill 1386, FISMA
- Make sure that your vendors interoperate to meet these standards
- Set clear security policies and publicize to all employees
- Drive user Human Behavior through social engineering
- Enforce through use of technology that audits, tracks and backs-up information on mobile devices

Dealing With Some Of The Major Concerns

Lost Data and Support Costs

- Despite your best efforts and security measures, data may be lost or stolen
- Minimize the damage done
- By issuing and enforcing company USB asset you can enable:
 - Forced Encryption to all USB drives
 - Recover Lost data that was backed-up
 - Remotely shred/destroy a drive if required
 - Manage access and provide Audit trail
 - Do not need to report if data on device was encrypted

Seven Key Steps to Remember

1. Always define and publicize your organization's policy for personal storage devices
2. Institute the use of company-issued personal storage devices
3. Make sure these devices are fully encrypted
4. Make sure users cannot circumvent security measures
5. Maintain an audit trail of data stored on devices
6. Be able to recover data residing on personal storage devices
7. Make sure your enterprise solution comprehensively provides the ability to control the use of all removable devices, inside and outside the corporate environment, and to centrally manage company-issued USB devices

Where is this Technology going?



Encrypted Storage with Two-Factor Authentication



The Security Division of EMC

Cruzer Enterprise and RSA SecurID

- The SecurID plug-in allows Cruzer Enterprise drives to generate one time password for two-factor authentication
- Combines secure storage and two-factor authentication
- Centrally managed - CMC and RSA server integration
- A solution to the "keychain" problem



Cruzer Identity

The combined power of smartcard-based security and hardware-based encryption

Two-Factor Authentication

- Smartcard-based access control to host PC and drive storage

Full Disk Encryption

- Full disk encryption application runs from the drive
- Encryption keys stored in smartcard memory as a private object

Encrypted USB Flash Drive

- 256-bit AES Hardware Encryption
- Mandatory security of all files
- “Lockdown” mode to prevent Brute Force password attack

Centrally manageable

- Complete lifecycle management with CMC



Smartcard Technology



Cruzer Identity Platform

- **Strong PKI-based two-factor authentication solutions for a variety of applications:**
 - VoIP, eBanking, copy protection etc'
- **Smart SDK to manage both smart card and storage resources**
 - Automated application compatibility with various operating systems
 - C++ based developer interface
 - Multiple applications support on a single device
 - CD and auto-run functionality
 - Streamlined integration between storage and smart card
- **Smartcard certification**

Secure, Managed, Virtual Workspace Anywhere, Anytime



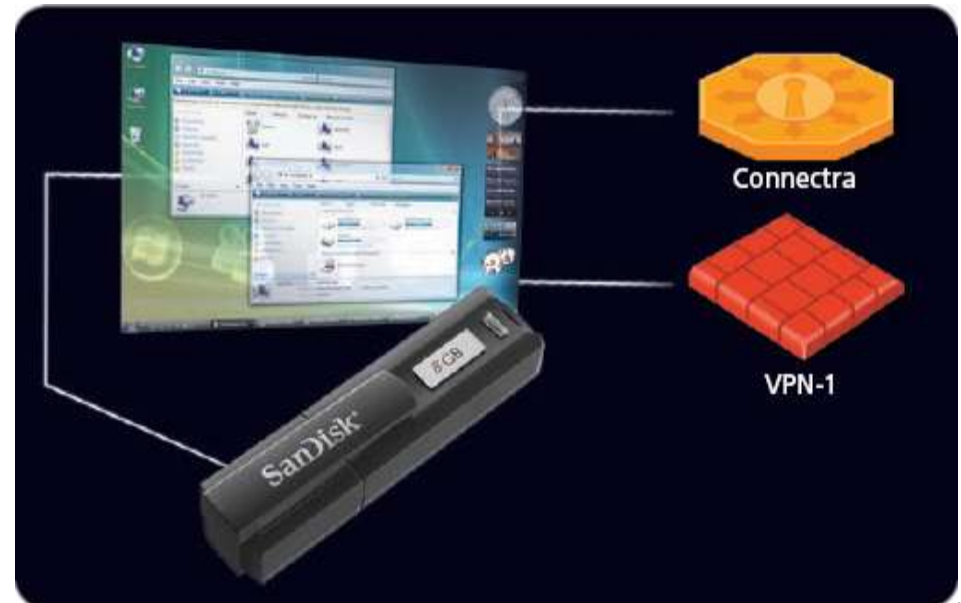
SanDisk & Check Point Joining Forces

- Best of breed
 - SanDisk enterprise-grade, managed USB flash drives
 - Check Point's Secure Workspace and VPN technologies
- Have your entire workspace with you on a secure UFD
- Access your workspace from any host PC
- Access your corporate applications even when offline
- Be protected from malware
- Connect securely to your corporate network



Secure Virtual Workspace for IT Professionals

- Provide employees with a consistent, controlled, encrypted and secure virtual workspace that is independent of the host computer
- Enforce mandatory access control on all files, stored in a hardware-encrypted, password-protected partition
- Centrally manage employees' workspace environments
- Apply granular security policies for different groups of users
- Enable compliance with privacy regulations
- Reduce TCO related to PC maintenance



Secure Virtual Workspace for Corporate Users

- Familiar work environment on host computers when plugging in SanDisk Cruzer Enterprise drive
- Pocket-sized drive with ample storage to transport all critical data and applications
- Ultra-fast data transfer speeds of up to 24MB/s Read and up to 20MB/s Write
- Access to corporate and IT resources through VPN (with optional two factor authentication)



Usage Scenarios

- **Day Extenders** who extend their office hours by working on the road and from home
- **Employees** who use business centers in hotels or transportation lounges
- **Consultants and guests** who are not permitted to take their own laptops onto a client's premises
- **Disaster recovery**



Summary

- **We deliver a comprehensive solution for data leakage, audit and control.**
- **Provide an end-to-end solution for securely mobilizing data using personal storage devices in the enterprise environment.**
 - Securely mobilize data using personal storage devices.
 - Enforce a policy on all removable devices and media.
 - Fully manage USB drives as company issued and controlled devices.
 - Minimize commercial and regulatory implications concerning lost or stolen sensitive information.

About SanDisk

- **Founded:** 1988
- **Public:** (NASDAQ: SNDK) November 1995
- **Notable Fact:** Worlds largest supplier of flash memory cards
- **Headquarters:** Milpitas, CA USA
- **R&D offices:** California, Israel, UK, India
- **Employees:** > 2600
- **Granted patents:** > 700
- **Annual Revenue:** > \$4.5 Billion
- **Market Cap:** > \$6 Billion
- **Patents:** 780 issued U.S. patents, and more than 400 foreign patents

Invented, co-invented or co-developed:

TrustedFlash
 U3 platform
 TransFlash (microSD)
 Memory Stick PRO Memory Card
 SD Memory Card
 MultiMediaCard
 CompactFlash Memory card
 PCMCIA Memory card
 USB Flash Drive

Also manufactures:

USB flash drives
 Smart cards
 SIM cards
 MegaSIM cards
 Embedded flash drives
 Solid State Drives

We deliver: Secure Business Mobility

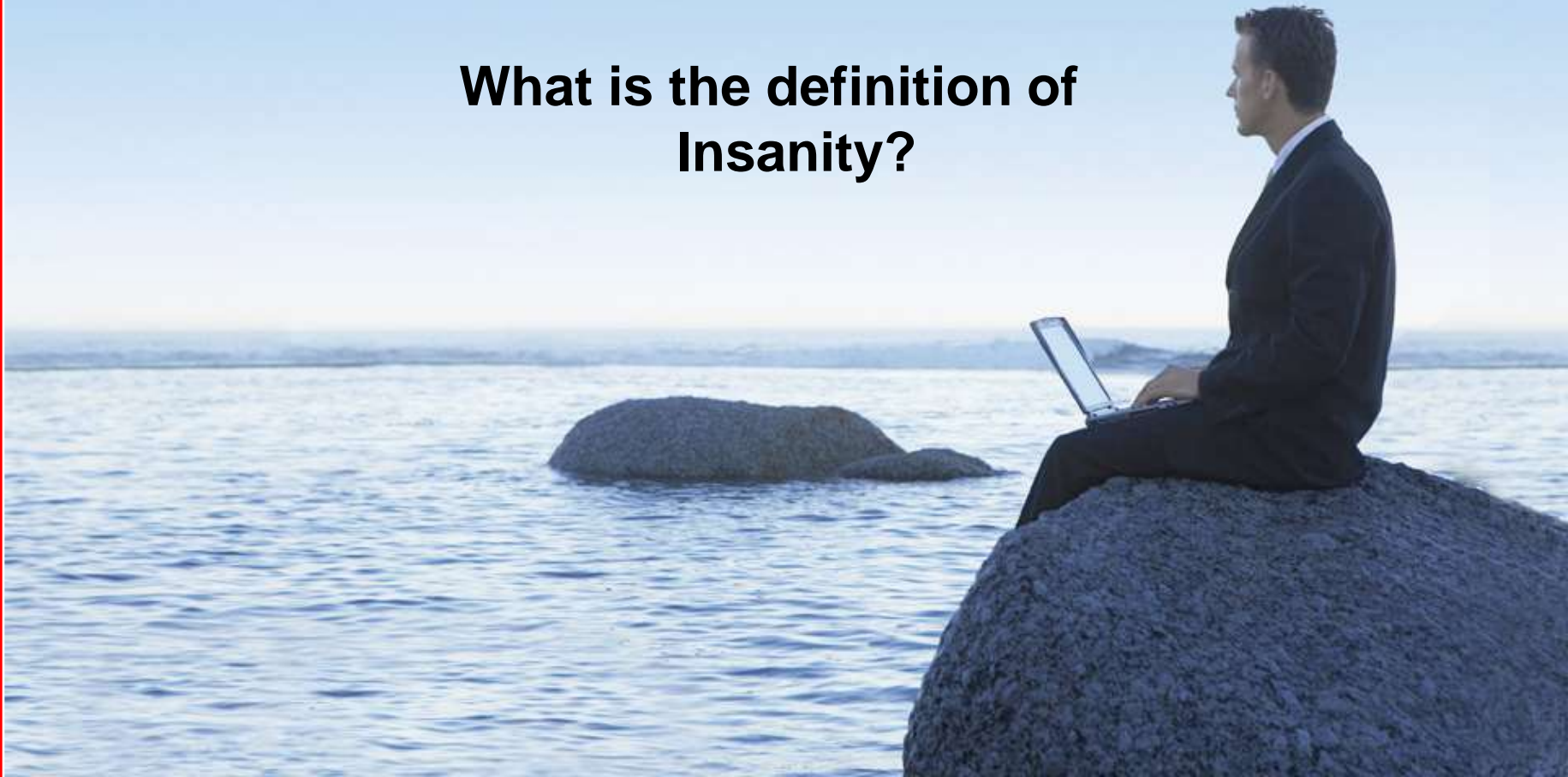
Mission Statement:

- To provide IT specialists with enterprise-grade solutions that bring together secure mobile storage, identity management and desktop virtualization, enhancing workforce productivity and mobility while allowing compliance and TCO reduction.

Closing Thought

Question

**What is the definition of
Insanity?**



Closing Thought

Insanity:

**Doing the same thing over
and over again expecting
different results!**

Albert Einstein

Brian Hawes
Sr Account Rep - Americas
Enterprise Division
(312.351.3227 - Office)
brian.hawes@sandisk.com

