

Agenda

DECEMBER 6, 2006 Section 1

8:30 AM – 9:30 AM Session 1.1 **Summit Overview and Current Legal Framework for Liability Associated with Data Loss**
Alan Paller, Director of Research, SANS; **Ben Wright**, Attorney
Agency chiefs have been blasted by members of Congress; corporate executives have been shamed in front-page newspaper stories; IT directors at universities have been fired outright – all because they lost sensitive data. This session provides an overview of the key questions executives are asking and the topics the Summit will cover. It also provides a summary of the laws, regulations and legal standards that mention encryption as a data security measure. This presentation will examine the extent to which the law rewards the use of encryption, or imposes penalties for its absence. Subjects include HIPAA, PCI, and the data breach notification statutes. Mr. Wright will offer practical tips on what to say and do regarding encryption.

9:30 AM – 10:40 PM Session 1.2 **Promising Practices in Selecting and Deploying Laptop Encryption — User Lessons Learned**
In this session, experienced users of the leading solutions discuss the processes they used to deploy mobile data encryption enterprise wide, and share the lessons they learned.

Lawrence C. Hale, ACS – ACS deployed PGP® Whole Disk Encryption to protect confidential information on corporate laptops. What regulations were relevant? What were the selection criteria for the solution, and why was PGP® encryption the better choice? What lessons were learned along the way?

Stephen Fried and **David Pom**, Metavante Corporation

Deploying Desktop Encryption with Utimaco SafeGuard Easy

Lessons learned from a fast-paced project to analyze, test, and deploy encryption to over 5000 laptop and desktop computers within a three-month timeframe, ultimately leading to the decision to deploy Utimaco's SafeGuard Easy encryption. This presentation will review the project from both the business side and the technical side. The business constraints and requirements that led to the use and selection of the product were often as difficult to navigate as the technical evaluation and deployment logistics. They will also review how project decisions affected the deployment as well as the technical challenges and successes.

James Summers, Vesta Corporation

Encryption for Tier I PCI Compliance

Vesta used nCipher nETHSM and wrote their own service that can be used by any of their applications to call into the nETHSM for encryption and decryption resulting in a universal encryption fix.

10:40 AM – 11:00 AM Break

11:00 AM – 12:15 PM Session 1.3 **Top Mistakes in Deploying Mobile Data Encryption — User Lessons Learned**
Once again, PC encryption users who have deployed mobile data encryption solutions enterprise-wide will share their experiences, but in this panel, they will focus on the major problems they faced, from key management to remote critical user support, and more.

T.J. Klevinsky and **Andrew Zolper**, JPMorgan Chase

Data Security on the Go: Lessons Learned from Encrypting 22,000 Laptops

Laptops have become standard equipment for today's workforce. The ability to work anywhere, anytime has transformed downtime to productive time. However, the risk/ tradeoff is increased possibility of lost equipment, data, and confidential information. JPMorgan Chase addressed this risk by rolling out boot-level hard drive encryption on all 22,000 corporate laptops. Andrew Zolper managed the deployment of this software and will cover the planning, implementation, and lessons learned associated with this project.

Tim McKnight, Northrop Grumman

Rolling Out Laptop Encryption: It wasn't as hard as we thought it would be.

In addition to sharing the lessons Northrop Grumman learned, he will debunk some of the catastrophe myths and talk about legal and export control issues.

Agenda

DECEMBER 6, 2006 Section 1 (CONTINUED)

11:00 AM - 12:15 PM Session 1.3 **Top Mistakes in Deploying Mobile Data Encryption — User Lessons Learned (Continued)**

Mark Lichtenberger, Northwestern Mutual

Successful Enterprise PC Full Disk Encryption: What are the business drivers to encrypt PCs?

How do you successfully implement hard drive encryption on more than 20,000 PCs across the enterprise (including 15,000 sales people)? What are the challenges before, during, and after? Can it be done with minimal negative impact on end-users? How long does it take? What are the “gotchas?”

Mel Stockwell, FDIC

FDIC's Top 5 Challenges to implementing a corporate-wide solution for Mobile Data Encryption

Valuable lessons learned regarding unexpected consequences of encryption and the employee impact, difficulties encountered in automated software deployments, residual security risks, coordinating multiple security implementations and complicated deployment processes.

12:15 PM – 1:30 PM Lunch

1:30 PM – 3:00 PM Session 1.4 **The Top Ten Things to Look Out for in a Laptop Encryption Deployment**

Eric Cole, SANS Instructor

There is a reason many organizations have still not deployed encryption: it is difficult. The good news is that other organizations have already made the mistakes, so you can learn from the pioneers and avoid the pitfalls. This talk will focus on things to avoid and on ways to make laptop encryption a business enabler, and as efficient as possible. Here are a few samples:

- *Key deployment* – Many organizations make the common mistake of focusing on products and algorithms. Understanding that strong encryption depends on key protection will help protect an organization from being compromised later.
- *Understand which risk is being mitigated* – Organizations often think that if they deploy laptop encryption, all of the data is protected, but they have to understand that it only protects data in transit. Other, complimentary tools may be needed to properly reduce the true risks.
- *Risk of attackers using encryption against you* – Encryption stops someone from reading information – that's usually good, but encryption can be used by attackers to stop legitimate users from accessing information. Therefore encryption must be properly controlled so it is not used against a company.

3:00 PM – 3:20 PM Break

3:20 PM – 5:00 PM Session 1.5 **Encryption Tools Today and Tomorrow**

This is your chance to compare the leading solutions by hearing senior strategists from the vendors presenting their stories. You'll have lots of time to ask them penetrating questions.

Warren Smith – GuardianEdge

Jon Callas – PGP Corporation

Jamie Barnett – RSA, the Security Division of EMC

Dave Anderson - Seagate Technology

Agenda

DECEMBER 7, 2006 Section 2

8:30 AM – 9:30 AM

Session 2.1

Window Vista BitLocker

Jason Fossen, SANS Instructor

Windows Vista introduces a new sector-level hard drive encryption technology named “BitLocker”. BitLocker not only provides whole-drive encryption, but also verification of the integrity of the boot-up environment if a Trusted Platform Module (TPM) is installed in the motherboard. In this presentation, we will discuss the requirements, advantages and disadvantages of BitLocker for securing your data when computers are lost or stolen. Because BitLocker is “free” with Vista and Windows Longhorn Server, and can be managed through Group Policy and command-line scripts, BitLocker will become a very popular and widely-used technology. Are you ready for it?

9:30 AM - 10:40 AM

Session 2.2

More Promising Practices in Selecting and Deploying Laptop Encryption — User Lessons Learned

Rhonda Maluia, Naval Special Warfare Development Group

On-Disk Encryption – Is it better than software encryption?

The discovery cycle including threat, protection, user knowledge and environment, research, hard drive encryption, findings, implementation scenarios.

Monty McDougal, Raytheon

Commercial vs Freeware and Problems Encountered

PGPdisk and TrueCrypt Solutions for un-planned reboots, the importance of backups, and free solutions.

Matt Norris, MicroMenders

The Decision Process: Is Backup Encryption Worth it?

How to make decisions and the financial case. Encryption at backup system level vs. encrypting data at rest. Tape backup encryption testing and deployment. Maintenance and auditing.

Edmond Comber, Rothschild

Lessons Learned While Deploying Safeboot

All laptops worldwide security encryption. The best lesson to learn with SafeBoot is to read the documentation and test the various options and parameters before you deploy. Rothschild chose the RIGHT product and had all our laptops worldwide securely encrypted with pre-boot authentication in a controllable and workable fashion. The motivation was not to be part of any ‘Laptop stolen, sensitive data accessed’ type headlines – reputation is everything!

Richard Goetz, Kronos

Currently involved in determining needs and securing laptops in the field and protecting data in the event of lost and stolen laptops. Richard will define the case for on-board encryption built into hard drives.

10:40 AM - 11:00 AM

Break

11:00 AM - 12:15 PM

Session 2.3

Tools Today and Tomorrow (Vendor Panel)

A discussion of current solutions and how they are evolving to address future issues in maintaining security and meeting regulations.

Steve Schmalz – RSA, the Security Division of EMC

Tim Stone – Stoneword

Jon Callas – PGP Corporation

Michael Willett - Seagate Technology

12:15 AM – 1:30 PM

Lunch

1:30 PM – 2:10 PM

Session 2.4

Encryption at Rest: Next Steps on Hard Drive Encryption

Jay James, National Security Agency/Information Assurance Directorate

This presentation covers the reasons to include recently enacted laws, the technology response, and the next steps to be taken by the U.S. government and industry.

Agenda

DECEMBER 7, 2006 Section 2 (CONTINUED)

2:10 PM – 3:15 PM

Session 2.5

Key Criteria in Selecting Secure Storage and Encryption Solutions

The Vendor Side of an RFP: Secrets to a Successful RFP Process

How does a vendor approach the RFP process? How can an RFP be structured to ensure you achieve your desired result? What is needed for successful communication with the vendor?

Jon Bazemore, PGP Corporation

Lee Day, RSA, the Security Division of EMC

3:15 PM – 3:30 PM

Break

3:30 PM – 5:00 PM

Session 2.5

Key Criteria in Selecting Secure Storage and Encryption Solutions (Continued)

The Requestor Side of the RFP

George Washington University, Encryption RFP Process

Alexa Kim, Executive Director, Technology Services

Krizi Trivisani, Chief Security Officer

George Washington University has recently completed the RFP process for to roll-out laptop encryption university-wide. They will share their experiences in the process and provide insights into what went well and what they would now approach differently.

Colorado Laptop Encryption RFP Process

Mark Weatherford, CISO, State of Colorado

Mike Weber, Security Engineer with Colorado CISO

Bob Feingold, Colorado Laptop Encryption Project Manager

The State of Colorado is currently going through an RFP process to secure a solution for state-wide laptop encryption. They will share the steps they have taken and the lessons learned along the way.

Procurement Standards Initiative

Alan Paller, Director of Research, SANS

An announcement of the goals and plans for a project to develop Secure Storage and Encryption Standards for software and hardware.

Evening Programs

The Summit includes both a unique opportunity for networking, and a rich set of programs to foster that networking.

- Secure Storage & Encryption vendor hospitality suites
- Security vendor “Lunch and Learn”
- Opportunities to ask more questions of Summit speakers.