



How it relates to "Data at Rest"

George McNeil IT Professional III (Security)
State of Nevada
Department of Information Technology
Office of Information Security



What is Data at Rest?

- ◆ Data at Rest is data that resides on your laptops, desktops, and mobile devices, (e.g. Personal Digital Assistants (PDA), Flash Drives, or external hard drives).
- ◆ Data at Rest is not data in a state of transmission.



The data may be at rest but the devices that it is stored on may not be. These devices are effectively exposed to all types of security risks.





It will never happen to me!

- ◆ Over 600,000 laptop thefts occurred in 2004, totaling an estimated \$720 million in hardware losses and \$5.4 billion in theft of proprietary information. *Safeware Insurance, 2004*
- ◆ 97% of stolen computers are never recovered. *FBI*
- ◆ 81% of companies reported the loss of one or more laptops containing sensitive information during the past 12 months. *Ponemon Institute, 2006*
- ◆ The chances of a laptop being stolen are 1 in 10. *Gartner Group, 2002*
- ◆ 70% of security incidents that actually cause loss to enterprises – rather than mere annoyance – involve insiders, and not cyberattacks. *Gartner Group, 2002*



I think I lost it

- ◆ Data loss has occurred everywhere in the United States. No one is exempt from a loss.
- ◆ Flash drives are particularly vulnerable to loss.
- ◆ Lost does not mean no one found it.
- ◆ A lost device can cause the “Data Steward” large headaches as they must notify the data owner.



Sixty percent of data breaches can be attributed to lost or stolen mobile devices. With this in mind, it is critical for State Agencies to bolster defenses by encrypting data on mobile devices.





Encryption

The process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.



Radio **Orphan Annie's** **Secret Society** **1936 Radio Decoder Badge**





Samples of what encryption is used for today:

- ◆ Credit Card Information
- ◆ Private correspondence
- ◆ Sensitive company information
- ◆ Social Security numbers
- ◆ Bank account information
- ◆ Personal Identifiable Information



NRS 205.4742

“Encryption”

“Encryption” means the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to:

1. Prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound;
2. Cause or make any data, information, image, program, signal or sound unintelligible or unusable;
or
3. Prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network.



NRS 603A.220 Disclosure of breach of security of system data

Any data collector that owns or licenses computerized data which includes personal information shall disclose any breach of the security of the system data following discovery or notification of the breach to any resident of this State whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.



NRS 603A.040

“Personal information”

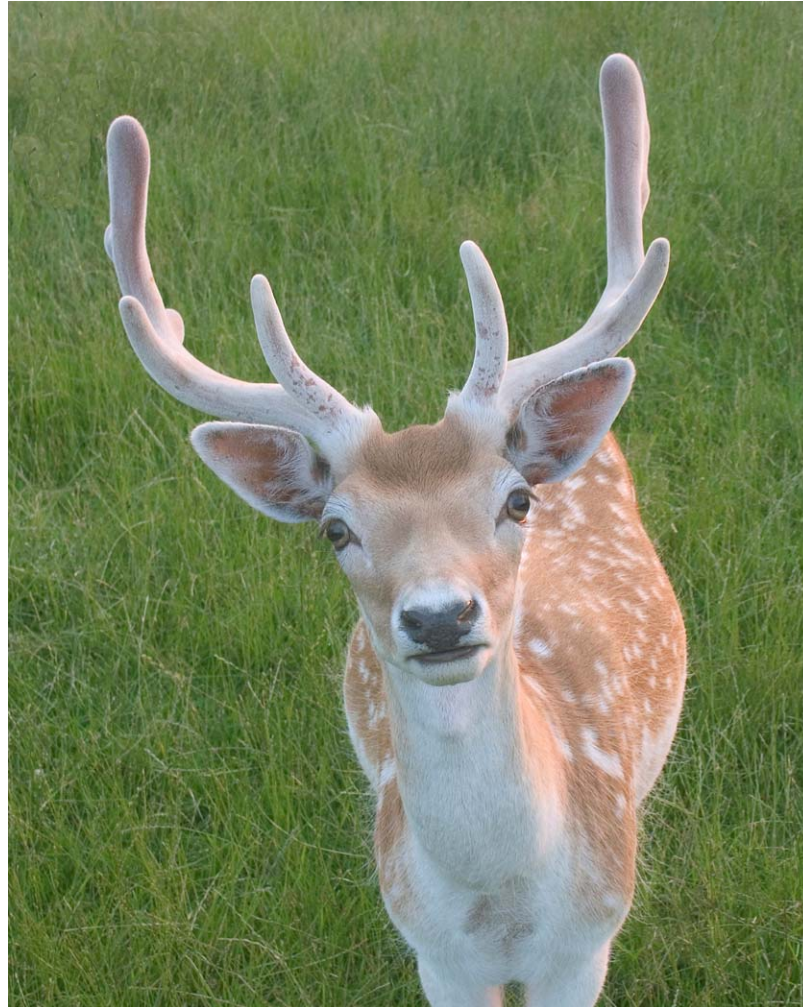
“Personal information” means a natural person’s first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted:

1. Social security number.
2. Driver’s license number or identification card number.
3. Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person’s financial account.

Note: The term does not include the last four digits of a social security number or publicly available information that is lawfully made available to the general public.



What can I do?





- ◆ Develop an Agency Mobile Device policy
 - DoIT Mobile Device Security Standard 54.02
 - http://inforec.intranet.nv.gov/security_PSPs.htm
- ◆ Limit or prohibit the use of portable devices
- ◆ Require encryption of portable devices
- ◆ Teach employee awareness of data responsibility
 - http://infosec.intranet.nv.gov/Security_Training.htm
- ◆ Know what is stored on the portable devices
 - ◆ Document it
 - ◆ Inventory it
 - ◆ Label it
- ◆ Classify the data, is it public or private



Free Encryption Software

- ◆ There are free on demand disk encryption or file encryption software packages that transparently encrypt files on your disk drive (or partition). On demand encryption tools allow the encryption of single files for those one-off occasions.
- ◆ Other software is available that can perform steganography, a sort of invisible encryption, where the plaintext version of your sensitive data is encrypted and hidden inside another file.



Hazards of free encryption software

- ◆ Does not support hierarchical keys.
- ◆ User can change key and lock Administration out.
- ◆ May use encryption algorithms that are weak.
- ◆ May have data size limitations



Proprietary Disk Encryption

GSA DAR Approved Vendors

- CREDANTMobile
- Data Armor
- GuardianEdge
- Pointsec
- Safeboot Device Encryption
- SafeNet ProtectDrive
- Secret Agent
- SecureDoc
- DS Data Security Suite
- Skylock At-Rest
- Talisman



Contact Information

George McNeil IT Professional III (Security)

State of Nevada

Department of Information Technology

Office of Information Security

e-mail: infosec@doit.nv.gov

phone: 775 684-7348

website: www.infosec.nv.gov