Matching security to data threats - more can be better, but less is bad

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- What are the threats to data
- How much of it needs to be secured
- Where do these threats come from
- Where is data accessed from
- What solutions are there today

Threats to structured data

- Raw structured data is typically not very useful without the application schema and all the tables
  - Many databases provide column level encryption for critical data
- Reports and extracts can usually be saved externally
  - Local storage, USB devices
    - Email, dropbox, Fax
- Some applications provide access control, local save prevention, etc.
  - But not all
- Once extracted, the data is essentially now file data

Threats to unstructured data (files)

- Physical removal
  - Repair of drive arrays
    - Annualized Failure Rates of 8.6% for 3yr old drives (1.7% new drives)^
      - For 1000 drives = 17 failures 1st year, 86 failures 3rd year
  - Loss or theft of hardware
    - Laptops
    - Servers (outside the main datacenter)
- Copying and subsequent misuse
  - Backups, Archives, DR sites
    - Unattended sites give plenty of opportunity for misuse
  - USB devices, paper copies, home backups, mobile backups
  - Email, DropBox, Fax, etc.

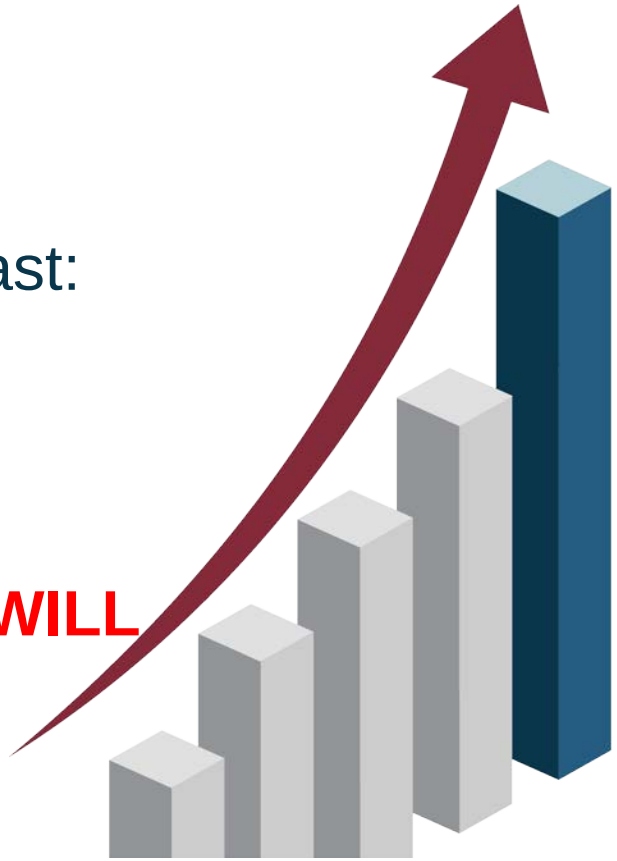
^Google 2007 study

Threats to unstructured data (files)

- Unauthorized access by Users
  - Simply browsing to places they should not be able to access
- Criminal access by Users
  - Targeted at specific data
- Unauthorized/criminal access by System Admins
  - Who need to have access for operational reasons
    - Backups, replication, etc.
- File Sharing
  - Can allow simple access to vast quantities of files
- The sheer size and growth of files

Unstructured data growth

- File-based storage (NAS) is exploding YoY:
  - IDC: 28%
  - Gartner: 36%
  - NetApp & EMC: ~30%
- Ethernet-attached storage growing fast:
  - iSCSI/NAS: 50% using it by 2014 (Gartner)
  - 27% in 2012
  - Using existing network architectures
- Problem is not going to go away—it **WILL** get worse



More can be better, but less is bad

What data needs to be secured

- Typically there are four categories of file data that need to be secured:
  - Classified Information
    - Governmental, Military, Intelligence - strict hierarchical schemes, etc.
  - Regulatory Compliance
    - Current: HIPAA, PCI, PII, etc. – binary – no shades of gray
    - Future ?: GDPR (General Data Protection Regulation), Right to be Forgotten
  - Confidential information
    - Intellectual property
    - Proprietary information
    - Competitive data, etc.
  - Anything else for any other reason
    - Whenever there is a need, whatever it is, good or bad!

Does it ALL have to be secured

- It depends on a number of factors:
  - Identification
    - Do you know where ALL your critical data may reside
  - Relevance
    - Is it possible to segregate relevant from irrelevant
    - Can you be sure you can identify ALL the relevant data
  - Quantity of data
    - Column level encryption
    - Tokenization / Obfuscation
    - Deduplication, Compression before securing
  - Impact of revelation, loss, or misuse
    - Can you afford the immediate cost
      - Monetary penalties, business restrictions
    - Can you afford the longer term cost of loss of reputation

Where do the threats come from

- From outsiders
  - Where the most money is spent by IT (~12% storage budget)
- From Insiders
  - System Admins
    - 82% according to FBI
    - Human Engineering

Perimeter security is ineffective

- Perimeter defenses are ineffective today according to security
  - 31
  - industry
- 59% said t meter breach occurred, high value data would not be safe
- 66% believe they will suffer a breach within the next 3 years

Show of hands:
Has your organization ever experienced a data breach?

* 2012 study by SafeNet Inc.

Why data security is needed

- 95% continue to invest in and employ the same data security strategies (Network perimeter security)
- 35% state they know their security investments are being deployed to the wrong technologies
- 20% would not trust their own personal data to their own networks

So what does all this mean?

- We have to accept that breaches WILL happen and once they do, the only protection is to secure the data itself
- **The new perimeter is the data itself – we must Secure the Data**

Where do the threats come from

- From outsiders
  - Where the most money is spent by IT
    - Not effective
- From Insiders
  - System Admins
    - 82% of all breaches according to FBI
  - Corrupt or idealistic employees
- Do you remember when …

More can be better, but less is bad

… Snowdon was just a mountain in Wales

Where is file data accessed from

- In main datacenter(s)
  - Application server
  - NAS/Fil… …ystem or shared
  - User
  - Ba… …lisk
  - Al… …sk
  - Vir…
    - …
- Managed fro… …rs
  - Cloud (Public, Private, Hybrid)
    - No different than backups and archives

Quick Show of Hands:

How many of you know the location of EVERY clone or snapshot of your VMs?

Where is file data accessed from

- Distributed locations, remote offices
  - App server
  - NAS server
  - User desktop

  Computer-local file system or remote file system in main datacenter over VPN
  - Backup device – local/remote tape or disk, external drives
  - Virtual Machines – when not running
    - Clones, snapshots

Where is file data accessed from

- Mobile – two types
  - User mobile device – local file system
    - Support for local apps may not be possible
    - USB dri[illegible]xt
  - Enter[illegible]
    - S[illegible]
    - [illegible]
- Mobile[illegible]ed down locati[illegible]
- Mobile dat[illegible]d rarely secured
  - Home backups, clo[illegible]kups, USB sticks, smartphones
- With BYOD, this problem goes exponential!

Quick Show of Hands:

How many of you make backups of your company data at home or on USB?

What threats exist against file data

Assuming that all critical file data is actually encrypted:

- Distributing to remote locations can expose centralized keys
- Distributing to mobile devices can expose data as well as keys
- Database reports and extracts
  - Written to desktops, mobile devices, removable storage, etc.
  - Data leakage when further distributed via email, etc.
- Data exposure to unauthenticated people
- System administrators posing as authenticated users
  - **80%+ of all actual breaches are internal**

More can be better, but less is bad

What threats exist against file data

- From Dark Reading (June 2013):
  - In a survey conducted by Avecto at the recent Infosecurity Europe conference, 41 percent of security professionals rated malicious insiders as their chief worry.
  - More than 30 percent of respondents said they have no policy in place for managing administrator access.
  - The most common threat comes from employees who download and install unauthorized software, without understanding the potential risks associated with their actions.

Distributed File Data – remote access

- File data in a central datacenter can be accessed remotely with a high level of security and auditability
  - VPNs, Two Factor Authentication, etc.
- Centralized access results in good access control, policy enforcement, auditing and reporting
  - Alerting essential for real time response and prevention
  - Auditing and reporting ssential for post mortem investigations and compliance evaluation
- End points can be authenticated in real-time
  - Varying levels of authentication depending on user, platform, location, information accessed ,etc

Distributed File Data - inbound

- Moving or copying file data from remote sites to datacenters can be managed with careful planning
  - Daily replication/copy to HQ over secure tunnels
  - Backups to HQ over secure tunnels
- File data can be re-encrypted as it arrives
  - Depending on policy, etc.
  - Key versioning and tracking necessary

Distributed File Data – outbound

- Moving or copying file data from a datacenter to a distributed or remote location is problematic
  - Cannot use same encryption key as primary file data
    - File data usually encrypted on a per-share or per-folder basis rather than per-file
    - In any case, file must be duplicated and encrypted with a different key before sending
    - Means the key management system must track multiple keys per file (like versioning) to support secure destruction
  - Once file data is remote, access and auditability is a problem
    - Key exchange with remote location exposes key
    - Any offline access to the file bypasses real-time authentication
  - Detecting file data changes when file is returned to datacenter
    - Results in multiple copies of file data
      - with multiple keys

More can be better, but less is bad

Mobile File Data – even more problematic

- Moving or copying file data from a datacenter to a mobile device is even more problematic:
  - Loss of mobile device
    - Can be mitigated with FDE (Self Encrypting Drives)
  - No control over who, when or where data is accessed
    - Only if online authentication is mandatory (not possible in many situations)
  - Pre-upload is normally required
    - Copy files onto device before leaving for business trip
    - Means keys must also be pre-loaded
  - Duplication of file data to same or alternate mobile devices
    - Including keys
  - Saving of cleartext file data to removable devices

Conclusions

- We need to accept that network perimeter breaches WILL happen – the new perimeter is the data itself
- Different file data categories need different protection schemes – sometimes there is overlap
- An insider is your biggest threat for large data breaches (but you must also protect against intrusion)
- Mobile devices pose the biggest management challenges
- A centralized reporting and auditing capability is important
- A centralized alerting capability is essential
- File encryption alone cannot succeed without fully integrated authentication, access control, and Enterprise Key Management
- **We must Secure the Data as well as the networks**

Thank You

Questions, follow-ups, etc to:

Chris.Winter@safenet-inc.com

Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

Authorship History

Chris Winter - September 7th, 2013

Updates:

Additional Contributors

Please send any questions or comments regarding this SNIA Tutorial to
tracktutorials@snia.org