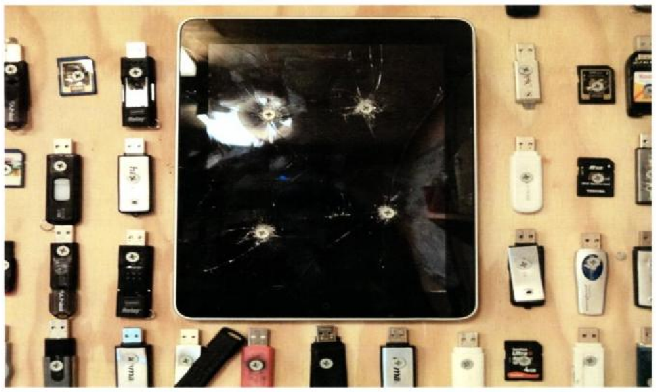
Securing Data and Handling Spillage Events

What Is a Data Spill and Why Is It a Problem?

Loss of control over sensitive and protected data by organizations is a serious threat to business operations and national security. In recent years, attackers have exfiltrated over 20 terabytes of sensitive data from Department of Defense, defense industrial base, and civilian government organizations. Malicious attacks are alarming, but more often spillages occur from unintentional user error or negligence.



Data spillage is the transfer of classified or sensitive information to unaccredited or unauthorized systems, individuals, applications, or media. A spillage can be from a higher level classification to a lower one. The data itself may be residual (hidden) data or metadata. Spillage may result from improper handling of compartments, releasability controls, privacy data, or proprietary information.

The trend towards increased information sharing has weakened access controls, giving users without a need-to-know access to large volumes of sensitive or classified data. Malware that propagates via removable media has increased the risk of large data transfers outside the network. The risk of data spillage is a problem largely because of inadequate end user security awareness, unmanageable networks, and poorly implemented data policies.

Security Recommendations

Ensure the Network Is Manageable

Network security begins by having a manageable network. The NSA's Manageable Network Plan is a series of milestones designed to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. It provides overall direction, offers suggestions, calls out crucial security tips, and gives references to books, web resources, and tools. (The Manageable Network Plan is a practical implementation plan for the NSA's Community Gold Standard, which gives a holistic view of the IA capabilities necessary to provide full-spectrum protection and defense for organizational enterprises.)

Establish and Enforce Data Protection Policies

Data protection controls help prevent unauthorized access, modification, destruction, and disclosure of data at rest, in use, or in transit. Secure baselines, such as the DISA STIGs or USG Configuration Baseline (USGCB) should be set for all workstations, servers, and network devices. Network hardening helps by configuring and managing user privileges, removing unwanted user accounts, closing unused ports, enforcing password policies, removing unwanted applications/services, and patching known vulnerabilities. Perimeter protection adds measures such as Intrusion Detection/Prevention and firewalls. Network software can work with other measures to prevent exfiltration of data. Adequate end user security awareness and training is essential.

Data at rest, on stationary or mobile devices and removable media, can be protected by full disk or file-based encryption. Access control should be enforced based on need to know. Use appropriate defenses to prevent malware on removable media.

Data in use can be protected by persistent enforcement of dissemination and use restrictions, protection from processes outside the application, and access control, to ensure that only authorized processes can access data sets and authorized memory spaces. Application whitelisting, which allows only authorized software to be run, helps to prevent malware and dangerous scripts from executing.

When feasible, data in transit is protected through encryption, data tagging (automated mechanisms for data marking and verification), or trusted path. Network monitoring tools should analyze all outbound traffic looking for anomalies, large data transfers, persistent or often-repeated connections, and unusual protocols/ports. These tools should block sensitive information leaving the organization and detect any unauthorized use of encryption, which may be used to bypass network security.

Integrity checks should be performed before and after use, transfer, or backup of data. Data integrity is verified through one-way cryptographic hash functions, digital signatures, and cryptographic binding.

Implement Data Loss Prevention

Data Loss Prevention (DLP) refers to a comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter. DLP is highlighted in the SANS Top Twenty Critical Controls: Critical Control 17, which lists ten recommendations on how to implement, automate, and measure DLP effectiveness. Data Loss Prevention falls under three broad categories:

- Network-based DLP, typically installed at the corporate gateway to scan network traffic such as email, instant messaging, FTP, web-based tools (http or https), and peer-to-peer applications for leaks of sensitive information.
- Host-based DLP, typically installed on desktops, laptops, mobile devices, USB drives, file/storage servers, and other types of data repositories to provide data discovery and classification capabilities and to identify and prevent leaks of sensitive information.
- Discovery DLP, designed to seek and find sensitive information on desktops, laptops, file servers, databases, email repositories, and within web content or applications.

After Incident "To Do" List

Assess, Report, Isolate, and Contain

All organizations should have a written policy on how to handle data spills, preparing a response team ahead of time and acquiring the necessary tools and resources.

When there is suspicion of a possible data spillage, first assess if a spill has actually occurred, the sensitivity of a potential compromise, and the users, systems, and applications involved. Report the incident immediately to the Information Owner, Information Security officials, and the responsible Incident Response Center. Report spillage of classified information in accordance with DOD 5200.01, vol. 3, 21 Mar 2012, http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf.

Isolate and contain to minimize damage and preserve evidence that may be required for damage and risk assessment, law enforcement, or counterintelligence purposes. Identify all information hardware and software systems and applications affected, and execute approved procedures to ensure that spilled data does not propagate further.

Affected media/devices take on the classification level of the compromised data until response team personnel have assessed the situation and executed appropriate procedures. If classified information appears in the public media, do not make any statement confirming the accuracy or classified status of the information, or discuss it with anyone without an appropriate security clearance and need-to-know. It is possible that verification of a compromise and the resulting damage assessment may result in a classification downgrade of all or part of the data.

As with any incident, if deliberate compromise of classified or sensitive data, violation of criminal law, or involvement by foreign intelligence agencies is suspected, report to appropriate authorities, in accordance with DOD 5240.4, 2 Feb 2009, http://www.dtic.mil/whs/directives/corres/pdf/524004p.pdf. If it is determined that a weakness or vulnerability in policy or procedures contributed to the compromise, the responsible security official should promptly issue new or revised guidance as necessary to resolve the identified deficiencies.

Sanitization and Recovery

The Authorizing Official (e.g. Designated Approving Authority) shall provide guidance and approve specific methods and products for systems under their authority. When authorized, execute approved sanitization procedures using approved utilities to permanently remove spilled data from contaminated systems, applications, and media. Use clean backup media, documentation (i.e. System Security Plan), and approved procedures to recover and restore all affected information systems and applications to an accredited, secure configuration. Additional guidance for sanitizing, destroying, or disposing of contaminated media includes:

- Guidance on high-security disintegrators, optical media destruction devices, high-security crosscut paper shredders, punched tape destruction devices, and degaussers: http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.
- NSA/CSS Manual 9-12: Storage Device Declassification Manual, 13 Mar 2006, http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf.
- Data Spill Procedures Guide for BlackBerry Smartphones, 24 May 2011, http://iase.disa.mil/stigs/a-z.html.
- Further guidance for sanitization can be found in NIST SP800-88, Guidelines for Media Sanitization, Sep 2006, http://csrc.nist.gov/publications/PubsSPs.html.

Data Spillage References:

- Manageable Network Plan, http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf.
- Defense Against Malware on Removable Media, http://www.nsa.gov/ia/_files/factsheets/Mitigation_Monday_3.pdf.
- SANS 20 Critical Security Controls – v3.1, Critical Control 17: Data Loss Prevention, http://www.sans.org/critical-security-controls/.
- NIST SP 800-53, Recommended Security Controls for Federal IS and Organizations, Aug 2009, http://csrc.nist.gov/publications/PubsSPs.html.
- Community Gold Standard – Data Protection, 30 Jul 2012, https://www.iad.gov/iad/CGS/cgs.cfm.
- CNSS Policy No. 18, National Policy on Classified Information Spillage, Jun 2006, http://www.cnss.gov/Assets/pdf/CNSSP-18.pdf.
- CNSS Instruction No. 1001, National Instruction on Classified Information Spillage, Feb 2008, http://www.cnss.gov/Assets/pdf/CNSSI-1001.pdf.
- CJCSI 6510.F, Information Assurance and Support to Computer Network Defense, Section C-49, 09 Feb 2011, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf.