Interested in learning more about security?

SANS Institute InfoSec Reading Room

Data Leakage Landscape: Where Data Leaks and How Next Generation Tools Apply

SANS ANALYST PROGRAM

Sponsored by Utimaco and Trend Micro

Data Leakage Landscape: Where Data Leaks and How Next Generation Tools Apply

A SANS Whitepaper – April 2008

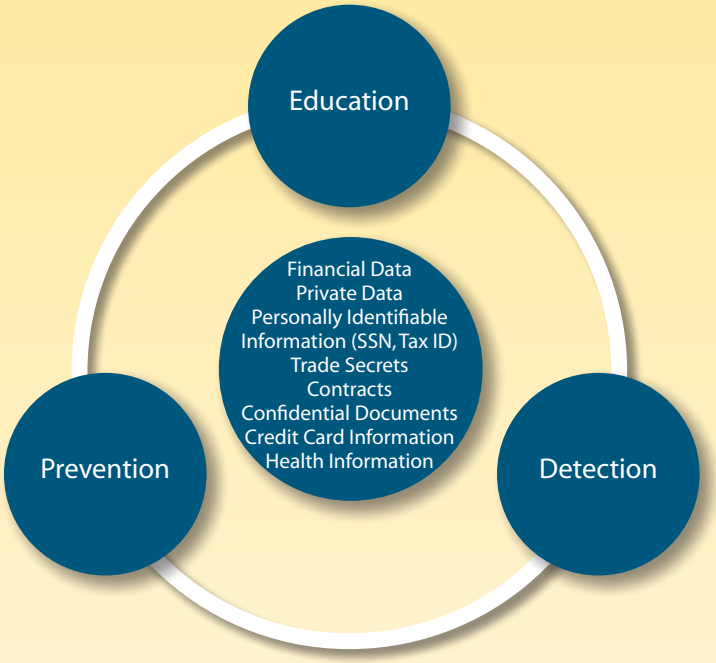
Written by Barbara Filkins & Deb Radcliff

The Leaking Faucet

Everyone is familiar with the concept of a data breach — confidential information, usually personally identifying information, falls into the wrong hands, and then suddenly, the data handler becomes reviled as the next TJ Maxx.

Data protection programs at most organizations are concerned with protecting sensitive data from external malicious attacks, relying on technical controls that include perimeter security, network/wireless surveillance and monitoring, application and point security management, and user awareness and education.

But what about inadvertent data leaks that aren't so sensational, for example unencrypted information on a lost or stolen laptop/USB or other device? Like the steady drip from a leaking faucet, everyday data leaks are making headlines more often than the nefarious attack scenarios around which organizations plan most, if not all, of their data leakage prevention methods. However, to truly protect their critical data, organizations also need to plan a more data-centric approach to their security programs to protect against leaks that occur everywhere sensitive data lives, rests or is used.



What type of protections would be required for, say, a training site for hospital call center employees, where actual lab reports and other real patient data are posted in the online training forms? How do you implement the same controls around data being cut/copy/pasted and e-mailed or sent out of the organization by other means?

Indeed, there are so many places data can easily leak out of an organization it would be difficult to note them, let alone classify and manage them, without some type of map or landscape that lays them all out. Broadly, these data leak points include:

- Sensitive data inappropriately removed, transferred, or sent out via postal mail, e-mail, Web mail, file transfers or instant messaging
- Lax, improper or missing access controls to systems containing sensitive data, from back-end databases and servers to mobile computers

- Lost or stolen computers, laptops and mobile devices with sensitive data that is unencrypted; hard disks and portable storage (CDs, USB drives) or backup devices; and paper files
- Insecure transmission of personal identifiable and other restricted data
- Authorized insider abuse of databases and other back-end systems
- Insecure or improper destruction of information, encompassing both physical locations (dumpsters) and electronic media (laptops and backups)
- Re-use of electronic resources (laptops and backup devices)
- Lack of separation of duties and access controls on databases and other shared systems

In this paper, we map these leakage points with regulations and best practices. Protection mechanisms can be simplified by breaking them into five major categories: classic malware protections to prevent system infections, enforceable access controls, encryption, filtering for data sensitive data types being sent out of the organization, and education.

In addition to traditional malware defenses, encryption and access controls play a huge role in protecting sensitive data from insiders no matter where the data rests or how it being acted upon. Equally important is the ability to filter, log, and take action on outbound traffic and downloads, which is commonly referred to as Data Leakage Protection (DLP). The last piece, education, can be enforced by the actions of the control systems themselves. For example, automatic encryption policies on some types of program actions (e-mailing, Instant Messaging, FTP usage) are already taken for granted by employees in many enterprises. And DLP control tools are well-positioned to send out educational pop-ups to users when their actions are actual violations.

Wrapping all this up with centrally-managed end-point security makes the neatest package for tackling the end-point related leakage problems, which is where much of the leakage occurs as a result of end user behaviors. Already, we're seeing convergence of some or all of these technologies from end-point protection vendors. However, it will be a while before organizations are willing to turn over their best of breed point solutions for a single product. Not to mention there are other considerations that these technologies can't manage, such as physical security issues related to lost disks and backups. But even under these circumstances, data can at least be rendered unreadable through encryption policies that are enforced by DLP at time sensitive data is downloaded onto the device in the first place.

Data Leakage Regulatory Landscape

Since July 1, 2003, when the California law SB1386 went into effect, the volume of proposed legislation to protect an individual against a potential data breach has soared. Most events that find their way to the Privacy Rights "chronology of breaches" list are sure to have violated some point of one or more of the major compliance regulations. So, instead of including the implicit violations of each law and regulation as it relates to each type of data leak, we're providing an initial landscape of how these laws relate to data leakage overall (see following Regulatory and Data Leakage table).

The impacts of loss of identifiable data can range from loss of reputation to severe financial complications and increased monitoring requirements and regulatory fines — not to mention, they're expensive. An information security breach may cost from $90 to $305 per lost record, according to a 2007 study by Forrester Research. Forrester, which notes that estimating the cost of breaches is an inexact science, based its figures on a survey of 28 companies who had some sort of data breach. They included legal fees, call center costs, lost employee productivity, regulatory fines, loss of investor confidence and customer losses to estimate these figures.

The following table compares the top data protection regulations with data leakage implications. Then, the next section aligns the data leakage points, themselves, with recommended best practices.

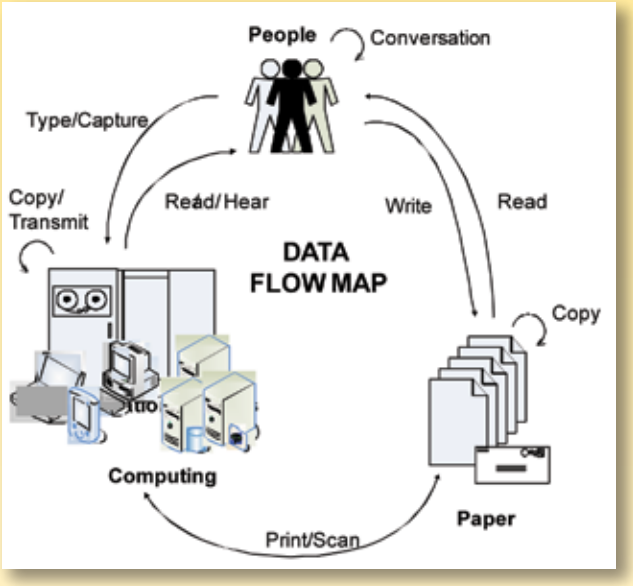
Regulatory and Data Leakage Landscape

Regulation	Focus	DLP Implications	DLP Recommendations
PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI/DSS) ***(International)***	Protection of payment card data and related consumer/business details during processing, transmission and storage	A widely-adopted set of specific technical and policy controls around implementation, assessment and audit of systems transacting financial data	Institute auditable DLP controls for data at rest and in transit, including encryption and detection of unencrypted payment card data. Block or log mass quantities of sensitive data, even when encrypted. Controls must be auditable.
GRAMM-LEACH-BLILEY ACT (GLBA) ***(United States)***	Protection of consumer nonpublic personal information (NPPI) data in financial services industry	Administrative and cryptographic processes for protecting data at rest and in motion, including physical safeguards	Locate/monitor mass quantities of personally identifiable data in motion with DLP filtering. Use encryption, where applicable, as well as strong access controls, all of which should be auditable.
SARBANES-OXLEY ACT (SOX) ***(United States)***	Protection of sensitive data related to financial reporting in public companies	Provides guidance for public companies in designing and reporting on the controls in place for protecting financial information	Utilize access controls, encryption, DLP fingerprinting or keyword analysis filtering for potential violations of disclosure of financial information.
EURO-SOX ***(European Union)***	Protection of sensitive data related to financial reporting in public	Requires mandatory encryption for financial reporting data and other related sensitive information at rest, in transit, and during processing	Institute encryption, encryption management, and endpoint security controls. Employ DLP content filtering, such as fingerprinting or keyword analysis, to monitor potential violations of disclosure of financial information.
HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA) ***(United States)***	Protection of electronic patient healthcare data and information (Note: Works with HIPAA Privacy)	Provides specific recommendations for access control, risk analysis, data disposal and re-use, data encryption (addressable), policy and documentation requirements	Use access control policies that follow data instead of operating solely at the system level. Employ encryption and DLP filtering for patient privacy data such as names, medical and financial keywords. This system must be auditable.
CALIFORNIA SENATE BILL 1386 (SB 1386) ***(United States)***	General protection of individual's private information	Foundation data breach legislation that has prompted similar legislation at all levels Unencrypted electronic, sensitive data is subject to the disclosure provisions	Utilize DLP filtering, encryption, strong access controls, endpoint management and other reasonable security controls.
DATA PROTECTION ACT (DPA) OF 1984 (AMENDED 1998) ***(United Kingdom)***	Handling of personal information for all UK industries and businesses	Deals with proper disclosure, rights of access to information, transmission and processing, and proper protective measures No specific technical measures mentioned	In addition to access controls, encryption, VPN / secure transport, filter for outbound personal information types and implement prevention.

Plug Leaks, Stem the Flow

Essentially, there are three buckets or containers where information "lives" — in digital form, in hardcopy (paper), and in the conversation and heads of people (see the figure below). Information is constantly flowing between these containers, usually resting in more than one of them at any given moment.

Data leaks can occur anywhere along these paths. So, ultimately, effective leak management requires not only the control of information and data at rest and in use/motion, but also a strong focus on the owners and users of information. Using the tenants of education, detection and prevention, a common set of best practices applies to all points of leakage. These include locating your data, mapping its usage, and then building protection policies and controls around the leakage points and user actions.



For most leaks, the following strategic global groupings of best practices, when used together, will allow organizations to guard against data leakage regardless of where the leaks tend to occur. These include:

1. **Handling Data According to Classification and Culture:** Environment affects how data is handled. To stem data leakage, you need to know both the type and form of sensitive information, where it resides, and most importantly, how it flows in your organization. Develop a data map for both data in motion and at rest. Identify the points most susceptible to data leakage. Once you have this picture for your organization, you can figure out how to handle information and data most effectively to mitigate leakage and to minimize any negative effect on your organizational culture.
2. **Design Your Employee Training Program with Experience in Mind:** Design your employee training programs to educate staff on patterns of prevention and develop needed self-awareness — the recognition of sensitive data, its transfer/delivery via e-mail, snail mail (what's this Social Security number doing on our mailer?) or IM. Employees need to understand the value of data and how it can be confiscated if handled incorrectly during storage/transport on physical devices and media. Reinforce education with Data Leak Prevention. Incorporate informational popups, reporting (when thresholds are met) and directions to more education on the subject matter the user is being warned about in the popup.

3. **Implement Controls for Detection and Prevention:** Develop controls and assign responsibility for enforcing data leakage policies, procedures and best practices:
   - **Administrative controls** include appropriate policies, guidelines and practices consistent with the application or the organizational environment. Don't look to develop blanket policies that lead to ineffective procedures. You will likely increase the potential of exposure rather than reduce it. Reinforce existing culture rather than hindering it.
   - **Physical controls** can include paper shredders, locking computer cases and biometric access. Don't shortchange the physical aspects of protecting sensitive data in your employee training and awareness efforts.
   - **Technical controls** will fall to traditional security tools coupled with today's more integrated endpoint and perimeter data protection controls, including encryption, outbound filtering and content controls to detect, report/audit, and prevent unauthorized downloading, e-mailing, copying or backing up onto portable devices.
4. **Create a More Holistic Security Environment:** Encryption to support enforcement applies just about everywhere, from e-mail to USB drives. The challenge is managing encryption across all the leakage points. Look for tools to make this task easier, including further convergence at the endpoint. As an added layer, outbound filtering tools for keywords, file types and other indicators of sensitive data leaving the organization through all endpoint leakage locations are emerging in the form of DLP tools. Further integrate with data lifecycle management practices, including secure data expiration (old e-mail and file purging) and storage.
5. **Adapting to Change is Not an Option:** Your information environment is constantly changing, so actively monitoring and adapting to change is mandatory. For example, other authorized users, such as business partners who hold or handle sensitive information, will need to prove they're also using the encryption and security standards you've laid out for protecting sensitive data. Under the Web services model, ensuring such compliance will become increasingly problematic. Growing reliance on wireless technologies, portable storage devices, and mobile access to corporate data over smart phones are also emerging technology changes that will require upgrades to your leakage prevention plans. Extend your security-monitoring program beyond the events occurring within your organization and watch industry and consumer trends for their implications, impacts and new risks to your sensitive data types.

Data Leakage Landscape 1:
Data in Use and in Motion

POTENTIAL REGULATORY VIOLATIONS

- **Perimeter security rules not established (e.g., PCI/DSS firewall)**
- **Data in transit not encrypted (PCI/DSS, GLBA, SOX, HIPAA, SB1386)**
- **Physical access to sensitive data not restricted (PCI/DSS, HIPAA)**
- **Media tracking system not in place (HIPAA)**
- **Unique identifiers not assigned for authorized users (PCI/DSS, HIPAA)**
- **Vendor-supplied default not changed (e.g., PCI/DSS)**
- **Administrative controls not adequate or enforced (GLBA, HIPAA, Privacy Regs)**

Databases and Other Shared Systems

Data Leak	Recommended Practices
A senior database administrator at a Certegy Check Services, a subsidiary of Fidelity National Information Services, was responsible for defining and enforcing data access rights at the company. He took data belonging to about 2.3 million consumers and sold it to a data broker. July 2007 *(CSOOnline)*	• Provide for Separation of Duties (SOD) between technical control users. Administrators of databases should not have access to the data in the fields and columns or access to the cryptographic keys protecting this data. • Use strong access controls and multi-factor authentication, again, minding SODs. • Enforce encryption and usage rules through DLP by tagging specifically protected data and file types, using keywords and other means, and filtering traffic and downloads outbound for signs of policy violations.
Jérôme Kerviel's ability to access systems he shouldn't have been able to led to the loss of $8 billion in bad stock trades, a hit so large analysts claimed its ripple effects could be felt across the world's stock markets. January 2008 *(multiple reports)*	• Enforce Separation of Duties on a technical level. No one person in accounting, for example, should be able to write and authorize checks. Similarly, no trader of a certain level should have access to higher level data and its applications. • Encrypt sensitive data in databases, again minding SOD with administrators. • Use database access controls, combined with endpoint DLP to monitor access to sensitive data in accordance with regulatory rules.

E-mail

Data Leak	Recommended Practices
One of Eli Lilly & Co.'s outside lawyers at Philadelphia-based Pepper Hamilton had mistakenly e-mailed confidential Eli Lilly discussions to *Times* reporter *Alex* Berenson (instead of *Bradford* Berenson), costing Eli Lilly nearly $1 billion. January 2008 *(http://www.portfolio.com)*	• Encrypt critical business communications, sharing keys with trusted business partner exchanges. • Enforce policies for log, encrypt, report, deny, and educate employees with DLP. Thresholds can be set high enough that ordinary communications are not blocked randomly, but only when mass transfers of critical data types trigger violations.
Personal information and Social Security numbers of 561 Virginia Commonwealth University students were inadvertently included in two e-mail attachments. The information included names, Social Security numbers, local and permanent addresses, and grade-point averages. December 2006 *(http://www.privacyrights.org)*	• Filter all outbound e-mails and attachments for sensitive data, especially mass or bulk data. Thresholds can be set high enough that ordinary communications are not blocked, but mass transfers trigger violations. • Enforce similar policies for encrypt or deny rules for restricted data in e-mail or IM attachments.

Instant Messaging

Data Leak	Recommended Practices
A bug discovered that could unleash a series of attacks on an AOL Instant Messenger user, with the most serious side effect being a remote hijack by a hacker. October 2007 *(http://www.infopackets.com)*	• Implement endpoint security controls to protect against drive-by downloads of malicious code to browsers, IM, and e-mail applications on computing assets and mobile devices. • Filter IM communications for breaches of sensitive data resulting from malicious code using IM channels to send data out.

Postal Mail

Data Leak	Recommended Practices
Taxpayers in northeastern Wisconsin had their Social Security numbers exposed in a state mailing from the Department of Revenue. A folding error, apparently the result of a faulty machine, allowed the Social Security numbers to be seen through the clear address window of the envelopes. January 2008 *(http://www.privacyrights.org)*	• Educate data handlers to recognize personally identifiable information on mailers and to inspect envelopes, windows, and postcards for information inadvertently exposed. • Implement paper shredding and other physical policies to protect mail, copies and other forms of paper data with sensitive information.

File-Sharing Site

Data Leak	Recommended Practices
Lexmark employee data was inadvertently exposed, including Social Security numbers, dates of birth, names and addresses, when accessed by two unknown parties when the data was loaded to a company file sharing site. February 2008 *(http://www.privacyrights.org)*	• Implement general DLP filtering as a safety net against accidents that expose large quantities of privacy data being uploaded to the FTP site to begin with. • Utilize access controls and data encryption. • Know who has access to network folders or corporate data sharing sites before you put restricted data there!

Web Exposure of Live Data

Data Leak	Recommended Practices
The Kaiser Foundation Health Plan IT staff training Web site was found to contain confidential patient information, including names, addresses, telephone numbers and lab results. Because of delays in reporting and closing the breach, Kaiser was one of the first to be fined for violating HIPAA by the California Department of Managed Health Care (DMHC). March 2005 *(http://www.computerworld.com/securitytopics/security/privacy/story)*	• Implement general content filtering of all network traffic leaving the company from the endpoint (cut, copy, paste and post to Web site) as a safety net against accidental exposures. • Educate end users when they violate policy through DLP popup messages. • Policy, in this case, should enforce against use of actual sensitive data in test or development systems, or for training purposes.

Physical Access to Computer

Data Leak	Recommended Practices
A professor at Middle Tennessee State University left a computer unattended in the mass communication department. An unidentified person is believed to have used the machine to send spam e-mails. The computer contained the names and Social Security numbers of past and current students. February 2008 *(http://www.privacyrights.org)*	• Program an automatic system shutdown or lockout after a specified time, requiring user credentials (i.e., password/token/biometric reading) to resume operating the computer. • Use endpoint encryption to protect sensitive files and data types. • The person could have just as easily starting sending sensitive data. DLP would notice a lot of SSN data types suddenly being sent and would block the action.

Physical Transfer (Mail)

Data Leak	Recommended Practices
In an on-going series of similar mishaps, at least two more CDs that could leave thousands of people open to identity fraud have been reported missing by staff at HM Revenue & Customs. Missing in transit from tax offices of Tyne & Wear in Washington, the CDs contained "sensitive information" including national insurance numbers and dates of birth. They were sent to offices in London and are yet to be accounted for. November 2007 *(http:// business.timesonline.co.uk)*	• Establish media tracking procedures that can be enforced through audit that satisfies regulatory requirements. • Ensure all data copied to physical media is encrypted and the credentials needed to view the information are properly segmented and protected. • DLP can log, encrypt and/or prevent such mass quantities of privacy data from being archived to removable media against policy.

Network Remote Access

Data Leak	Recommended Practices
A vulnerability analysis at a major southern California hospital revealed that doctors were able to log into their hospital desktop computers from home via an Internet-available RDP connection (no VPN) and were able to view patient information over an unencrypted channel. October 2005 *(Private communication with author)*	• Strong authentication and encrypted communication channels should be required for all remote access users. • Institute DLP protections against outbound transfer of protected data from remote log-ins.

Wireless Breach

Data Leak	Recommended Practices
A Wall Street Journal article notes that: because TJX had an outdated wireless security encryption system, had failed to install firewalls and data encryption on computers using the wireless network, and had not properly installed another layer of security software it had bought, thieves were able to access data streaming between handheld price-checking devices, cash registers and the store's computers. Twenty-one U.S. and Canadian lawsuits seek damages from the retailer for reissuing compromised cards. May 2007 *(http://www.privacyrights.org)*	• Use the latest workable WiFi WAP-based security standards for wireless encryption and network segmentation. • Obfuscate (replace credit card numbers or other critical data types with XXXX) at point of intake. • Encrypt log-in credentials, point of sale and network data traversing from wireless endpoints. • In proper terminal configurations, use of DLP can protect data at point of sale terminals and enforce encryption rules.

Data Leakage Landscape 2:
Data At Rest and In Storage

STANDARD /REGULATION VIOLATION

- **Data not encrypted (PCI/DSS, GLBA, SOX, HIPAA, SB1386)**
- **No contractual greement with 3rd party to protect senstive data (PCI/DSS, GLBA, HIPAA)**
- **Administrative controls inadequate or not enforced (GLBA, HIPAA, Privacy Regulations)**

Lost or Stolen Devices	
Data Leak	**Recommended Practices**
A **desktop** stolen from an Administrative System, Inc. (ASI) office in Seattle contained names and sensitive information about customers or employees of several of the firm's clients: Continental American Medical, EyeMed Vision/Kelly Services Vision, and Jefferson Pilot Financial Dental. Personal details may have included name, date of birth, mailing address, and Social Security number, depending on the service being provided. February 2008 *(http:www.privacyrights.org)*	• Encrypt sensitive data on desktops and mobile devices (full-disk, boot-level encryption recommended). • Utilize DLP to regularly scan data-at-rest on endpoints for unencrypted sensitive data and proactively remediate violations. • Promptly report any suspected theft of organizational-related computing equipment to your IT security department, and to authorities.
Workers at Research in Motion Ltd. woke up to an e-mail full of expletives from an otherwise mild-mannered female employee. A thief had broken into her home, commandeered her **BlackBerry** wireless device and e-mailed the expletives to the mail list. July 2005 *(http:// www.washingtonpost.com)*	• Encrypt sensitive data and password protect devices. • Employ mobile device security and storage card encryption. • Be able to remotely overwrite file systems or destroy them altogether when someone tries to turn on a lost/stolen device. • Watch for DLP filtering tools to reach these devices in the near future.
A contractor lost a **laptop** containing unencrypted psychological screenings of 441 peace officer applicants. It was stolen from the car of a contract psychologist for the State of California. As a result, California will require all contract providers to undergo privacy training and to encrypt all sensitive information on personal laptops. January 2008 *(http://www.ihealth.org)*	• Contracts with 3rd parties that access your confidential data should include: mandatory training for handling sensitive data; encryption of your data; agreement to allow physical inspections; and sanctions for loss of data in conjunction with their support of your organization.

Kiosks and Business Centers

Data Leak	Recommended Practices
Social Security numbers and other personal information for almost 17,000 beneficiaries enrolled in Humana Medicare prescription drug plan were left on a hotel computer/kiosk in Baltimore after a Humana employee called the data up and neglected to delete the file. June 2006 *(http://www.pharmacychoice.com)*	• Establish rules for sending or downloading personal identifiable or sensitive information to insecure or unknown computers. This should include location-aware data protection, such as isolation from memory, and encryption. • Utilize layered enforcement through DLP at gateways to log and alert for en masse transfers of sensitive data to unknown computers.

Portable Media

Data Leak	Recommended Practices
Stockport Primary Care Trust (UK) reported a member of staff lost a **USB memory stick** containing data extracted from the medical records of 4000 patients. The data was being carried personally to avoid being sent by e-mail because they thought it would be more secure. Data consisted of NHS number, Stockport PCT identification number, first and second name, date of birth, sex, condition, GP code, practice code, and GP name. December 2007 *(http://www.bjhcim.co.uk/news)*	• Enforce policy on a content-sensitive basis through DLP including logging, alerting, encrypting, and blocking the download based on keywords, file types and other criteria. • Enforce mandatory encryption of all sensitive information that is downloaded, no matter the medium it is copied to.

Backup Storage

Data Leak	Recommended Practices
A backup computer **storage device** with the names and Social Security numbers of 500,000 state workers was stolen out of a state intern's car. June, 2007. *(http://www.privacyrights.org)*	• Encrypt all backup media, whether online or physical, tape or disk. • Use DLP to control what is allowed to transfer to backup media, as well as logging and encryption policies for those transfers.

About the Author

Barbara Filkins has done extensive work in system procurement, vendor selection and vendor negotiations in her career as a systems engineering and infrastructure design consultant. Based in Southern California, she sees security as a process that she calls "policy, process, platforms, pipes, AND people." Most recently she's been involved with HIPAA security issues in the health and human services industry with clients ranging from federal agencies (DoD and VA) to municipalities and commercial businesses. Her interest in information security comes from its impact on all aspects of the system lifecycle as well as its relation to many of the issues faced by modern society that are dependent on automation: privacy, identity theft, exposure to fraud, and the legal aspects of enforcing information security. She holds the SANS GSEC (Gold), GCIH (Silver, working towards Gold), and GHSC certifications.

Deb Radcliff, SANS Analyst Program Editor, is an award-winning writer who has covered information security and online crime since 1994. Her articles are carried regularly in *Computerworld*, *Networkworld*, *CSO*, *SC Magazine*, *The Register*, *CNN Online*, and other leading computing and business magazines. They're also translated into many different languages, cited in research and law journals, and used verbatim in college textbooks. As a speaker, she's addressed audiences on business radio stations in Vancouver and Los Angeles, West Point, H.O.P.E. (Hackers on Planet Earth) and elsewhere. Radcliff holds a bachelor's degree in journalism from San Jose State University, where she graduated with honors.

SANS would like to thank its sponsors:

Last Updated: October 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced