Mistakes Happen—Mitigating Unintentional Data Loss

日本語版も入手可能
www.isaca.org/currentissue

Nobody intends to lose data, but it happens. Often. Immature processes, inadequate tools and unaware users reveal themselves as the weak links. The growing saturation of technology in all areas of business and personal life diversifies the sources of unintentional data loss. Ever-changing laws continue to increase the risk and cost of noncompliance when unintentional data losses occur. The confluence of these factors raises the stakes for all security professionals. After reviewing today's landscape, security professionals can plan to protect tomorrow's data from risk.

Changing Landscape

Unintentional data loss occurs when confidential information leaves a corporation's boundaries without explicit approval by authorized personnel. Continuing innovation in areas such as the cloud and Internet of Things (IoT) reduces boundaries. Entrepreneurial companies start up new services, transmitting and storing data every day. The move to the cloud and the increasing usability of cloud services are accelerating the risk of potential data loss. End users purchase applications such as cloud enterprise resource planning (ERP) solutions without involvement from IT or IT security teams. Without end-user recognition, these actions create shadow IT departments. Shadow IT increases the risk of data transmission and storage outside of organizational standards and controls.

Corporations recognize the significant risk inherent in protecting data. For example, almost 20 percent of the risk factors listed in Alphabet Inc.'s (Google's parent company) 31 December 2016 10-K reflected data security risk.[1] Examples include:

- If security measures are breached resulting in the improper use and disclosure of user data, or if services are subject to attacks that degrade or deny the ability of users to access products and services, products and services may be perceived as not being secure. Users and customers may curtail or stop using the enterprise's products and services, and the enterprise may incur significant legal and financial exposure.
- Intellectual property rights are valuable, and any inability to protect them could reduce the value of an enterprise's products, services and brand. A variety

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2AnuPtm

Mike Van Stone, CISA, CISSP, CPA
Is the director of internal audit at Ionic Security. His diverse experience includes technology, financial, operational and compliance auditing with companies ranging from Fortune 5 to a growing technology start-up. He led international, integrated and cosourced audit teams on four continents and in two languages. Van Stone has published a disaster recovery and business continuity article for Infragard's Atlanta (Georgia, USA) chapter and presented on the following topics during ISACA® Atlanta Chapter meetings and annual conferences: auditing the cybercontrols behind physical security, auditing the software development life cycle and integrated auditing.

Ben Halpert
Is vice president of risk and corporate security at Ionic Security Inc. He focuses on educating and empowering today's digital citizens in the workplace, at schools and at home. He also champions cyberethics education for children from preschool through high school via Savvy Cyber Kids, a nonprofit organization he founded in 2007. As a trusted voice on cyber and physical security issues, Halpert has made numerous conference, radio and TV appearances. He has been featured in newspapers and magazines; and has published many articles on smart technologies, data privacy and cloud computing.

Enjoying this article?

- Read *What Does It Mean To Me? GDPR Data Protection Impact Assessments*. *www.isaca.org/gdpr-dpia*

of new and existing laws could subject the enterprise to claims or otherwise harm the business.

- Privacy concerns relating to technology could damage an enterprise's reputation and deter current and potential users from utilizing its products and services.

Data Loss Laws and Regulations

As reflected in Alphabet Inc.'s 10-K, data protection laws and regulations continue to evolve with the changing landscape. Countries, states, regions and industries across the world focus on data security. Key laws, regulations and frameworks include the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), US Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), US Gramm-Leach-Bliley Act (GLBA), European Union (EU) General Data Protection Regulation (GDPR), and the Basel Accords.

Noncompliance can be costly. For example, the US Department of Health and Human Services (DHHS) reported HIPAA program-to-date settlements of US $67,210,982 as of 28 February 2017.[2] However, GDPR noncompliance has the potential to surpass the fines of any of those programs. The GDPR was approved by the EU Parliament on 14 April 2016.[3] While enforcement does not begin until 25 May 2018, companies must plan for the changes now to avoid the potentially costly penalties. Key changes resulting from GDPR include increased territorial scope, clearer terms, 72-hour breach notification requirements, rights to be forgotten and privacy by design.[4]

The EU Data Protection Directive 95/46/EC set an unclear territorial scope, but its replacement, GDPR, applies to all organizations processing the personal data of data subjects residing in the European Union, regardless of the organization's location. EU's Parliament approved GDPR penalties up to the greater of US $20 million or four percent of the violating organizations's global revenue. With such severe penalties, GDPR will drive focus on implementing "appropriate technical and organizational measures in an effective way in order to meet the requirements of this regulation and protect the rights of data subjects."[5]

Organizations often establish organizational standards and controls to support compliance with laws and regulations, but GDPR will drive organizations to include data protection from the onset of system design to avoid data protection failures. In addition, data-centric controls that may have been overlooked in the past will need to be revisited by control owners.

Unintentional Data Loss

Internal employees and contractors are often the source of data loss. **Figure 1** lists by calendar year, DHHS's top five issues in investigated cases closed with corrective action.[6] Notably, technical safeguards barely make the list on an annual basis.

Figure 1—Top Five Issues in Investigated Cases Closed With Corrective Action

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2014	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2013	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary

Source: Department of Health and Human Services Office for Civil Rights, "Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year," USA. Reprinted with permission.

In addition to the emerging challenges, longstanding challenges such as employee loss of computers, Universal Serial Bus (USB) drives and mobile devices put data at risk. Employees enter incorrect email addresses, fail to lock their computers, inappropriately share data with unauthorized partners, use unsecured peer-to-peer messaging, and take high-resolution office pictures with sensitive equipment or data in the background. In this new landscape with opaque boundaries and more threats of unintentional data loss, security professionals must prepare for the needs of a datacentric future to meet contractual and legal protection requirements.

> "IN THIS NEW LANDSCAPE WITH OPAQUE BOUNDARIES AND MORE THREATS OF UNINTENTIONAL DATA LOSS, SECURITY PROFESSIONALS MUST PREPARE FOR THE NEEDS OF A DATACENTRIC FUTURE TO MEET CONTRACTUAL AND LEGAL PROTECTION REQUIREMENTS."

Mistakes happen. However, there are important lessons to be gained from the plethora of well-publicized data protection failures. The following are selected examples of unintentional data losses and their impact:

- **Shadow IT**—A physician's attempt to disconnect his personal server from a hospital's network exposed 6,800 patients' data to Internet searches. The DHHS settled the claim for US $4.8 million.[7]
- **Stolen laptop**—An April 2016 theft of a California Correctional Health Care Services unencrypted laptop from an employee's car resulted in the loss of the personal health information (PHI) of 400,000 inmates.[8, 9]
- **Lost USB device**—The Alaska Department of Health and Human Services lost a USB device containing Medicaid beneficiaries' health information, resulting in a US $1.7 million fine.[10]
- **Lost mobile phone**—The 2013 loss of a mobile phone compromised the protected health information of 412 patients at six nursing homes, which resulted in a DHHS fine of US $650,000.[11]
- **Social media, data distribution, third-party data rights**—A UK watchdog group determined that, over a three-year period, the UK National Health Service had at least 50 instances of data being posted on social media; at least 236 instances of data being shared inappropriately via email, letter or fax; and at least 251 instances of data being inappropriately shared with a third party.[12]
- **Email**—In April 2014, an employee at a risk advisor and insurance brokerage firm accidentally sent a spreadsheet to a large group of employees containing employees' names, email addresses, birthdates, Social Security numbers, employee identification numbers, office locations and medical insurance plan details. The company paid for two years of identity theft protection for 4,830 people.[13]
- **Asset disposal**—A New York-based health plan provider returned photocopy machines to a lessor without wiping 344,579 individuals' data stored on the machine.[14]
- **Instant messaging and online disclosure**—A software, data and media company accidentally uploaded more than 10,000 confidential private instant messages of traders to a public website during testing.[15]
- **Clicking on email malware**—Banking employees clicked on malware called Carbanak, allowing hackers to gain access to data necessary to steal more than US $300 million, per Kaspersky Lab.[16]

With an ever-growing list of methods through which

> COLLECTIVELY, THE GOVERNANCE PRACTICES FORM DEFENSE-IN-DEPTH STRATEGIES TO ADDRESS DATA CONFIDENTIALITY, INTEGRITY AND AVAILABILITY.

data have been unintentionally lost, this is just a partial inventory. Many of these incidents highlighted a lack of control maturity or user awareness. Organizations must strive to continuously improve processes and controls protecting data.

Common Data Protection Controls and Considerations

Most IT processes and controls have a direct impact on data security. **Figure 2** lists several key COBIT® 5 data protection governance practices.[17]

Collectively, the governance practices form defense-in-depth strategies to address data confidentiality, integrity and availability. These layers are intended to address internal, external, intentional and unintentional data protection threats. Some common data protection controls and considerations for data security planning follow:

- **Data classification**—Classification policies and procedures drive access management decisions and data protection controls. Classification categories are often influenced by laws, regulations and frameworks. By classifying data, practitioners can empower organizations to grant access on a need-to-know basis. Most organizations struggle in identifying data and data locations due to their sheer volume, exacerbated by the presence of shadow IT. The challenges inherent in the process were made clear in the photocopying machine asset disposal data loss example previously mentioned. Organizations produce volumes and volumes of data every day and are often reliant on individuals to ensure data are consistently and correctly marked. Identifying, classifying and protecting data by classification are covered under COBIT® processes IDs such as APO01.06, BAI08.02, BAI08.03, DSS05.02, DSS05.03, DSS05.04 and DSS06.06.

Figure 2—COBIT 5 Data Protection Governance Practices

Practice ID	COBIT Practice Name
APO01.06	Define information (data) and system ownership.
APO07.06	Manage contract staff.
BAI08.02	Identify and classify sources of information.
BAI08.03	Organise and contextualise information into knowledge.
DSS05.01	Protect against malware.
DSS05.02	Manage network and connectivity security.
DSS05.03	Manage endpoint security.
DSS05.04	Manage user identity and logical access.
DSS05.06	Manage sensitive documents and output devices.
DSS05.07	Monitor the infrastructure for security-related events.
DSS06.03	Manage roles, responsibilities, access privileges and levels of authority.
DSS06.05	Ensure traceability of information events and accountabilities.
DSS06.06	Secure information assets.

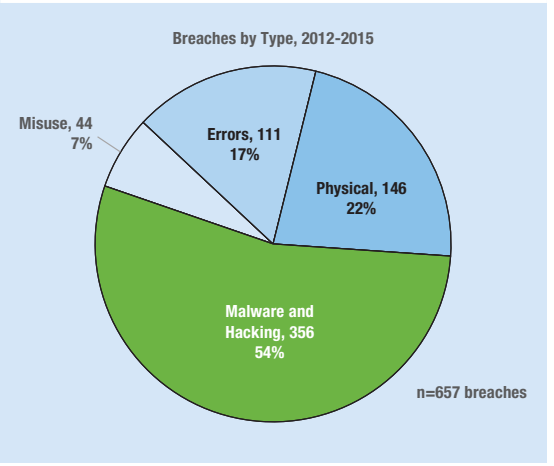
Source: ISACA®, *COBIT® 5 Implementation—Supplemental Tools and Materials*, USA, 2013. Reprinted with permission.

- **Data loss prevention (DLP)**—Ultimately, when marked or identified through rules, DLP tools can provide another layer of protection. Establishing data loss prevention rule sets requires careful planning and testing. If the rules are too restrictive, the tool becomes an impediment to business; if the rules are too permissive, data security is negatively impacted. DSS06.06 addresses the application of data classification policies and procedures to protect information assets through tools and techniques.
- **Encryption**—Organizations often apply encryption to data classified as sensitive. Data can be encrypted by multiple types of tools. For the previously noted data loss examples caused by asset loss, hard disk encryption may have mitigated the risk. However, hard drive encryption would not have helped with the examples in which the data left the hard disk and, especially, the network boundaries. File-level encryption tools add another layer of protection, but these tools have historically been hampered by insiders with knowledge of keys and passwords who retain access to the file. Additionally, difficulties in scaling key management effectively can limit enterprise-level implementations. As a result, end users often use consumer-focused file-level data encryption products that remain outside the scope of IT's centralized management processes, thereby creating further control weaknesses.

End users can often be the root cause of data losses. For example, the 2016 California Data Breach Report findings shown in **figure 3** reflect a common theme.[18] The errors category, totaling 17 percent of the breaches between 2012 and 2015, represents incidents stemming from anything insiders (employees or service providers) unintentionally do or leave undone that exposes personal information to unauthorized individuals. The chart also includes a physical category. This category includes both intentional thefts and unintentional hardware losses. COBIT covers encryption of information in storage and in transit according to its classification in DSS05.02 and DSS05.03.

- **User awareness**—Organizations build end-user awareness through policies, procedures, training and even phishing simulation tests. However, malicious actors continue to target employees to gain access to sensitive data. Building a security culture within an organization is necessary to drive higher compliance with procedures and gain full acceptance of security tools and monitoring. Former US White House Military Office Chief Information Security Officer Steve Pugh shared his method for gaining acceptance in this way: "I trust you, but I don't trust the packets coming from your machine."[19] This can be an effective cultural enabler to implement controls necessary to combat both unintentional and intentional data leakage. DSS05.01 emphasizes the importance of communicating malicious software awareness and enforcing prevention procedures and responsibilities.

Figure 3—California Data Breach Report Findings



Source: Harris, K.; "California Data Breach Report 2012-2015," California Department of Justice, USA, February 2016. Reprinted with permission.

- **Access management**—Properly addressing access management can be a difficult challenge. Most organizations deal with a constant flow of employees and contractors, a growing list of internally and externally hosted applications, and significant complexities in segregation of duties. Restricting access to files unintentionally distributed outside of an organization's network poses a significant obstacle to true end-to-end management

of access to data. Contractor access agreements, access reviews, access principles, access privilege assignment and segregation of duties are addressed in multiple processes, including APO07.06, DSS05.04, DSS05.06 and DSS06.03.

- **Logging and monitoring**—Logging and monitoring help detect security events and provide evidence to trigger the incident management process. Key challenges include monitoring third-party cloud applications accessible to employees from outside the corporate network and insufficient automation to effectively manage the large volume of log data. DSS05.07 concentrates on logging, level of log detail and log review.

> "FIREWALLS ARE STILL AN IMPORTANT PART OF ANY DEFENSE-IN-DEPTH STRATEGY, BUT THEIR SCOPE OF MITIGATION IS NOW MORE LIMITED."

- **Antimalware**—This software can often be required by contracts or industry regulations. However, over the years bad actors have become more savvy and intentionally develop hacks to evade common malware tools. This cat-and-mouse game continues to play out daily, but long gone are the days when antimalware software alone provided comprehensive endpoint and network protection. COBIT documents the standard to install and activate malicious software protection tools with updated definition files to filter incoming traffic and protect against unsolicited information in DSS05.01.
- **Firewalls**—These network security systems historically served as the castle walls effectively protecting data, but now, more than ever, data are leaving corporate networks by design and flowing to the cloud, partner connections and the multitude of consumer-managed devices introduced through bring-your-own-device (BYOD) implementations within organizations. In this changing landscape, firewalls are still an important part of any defense-in-depth strategy, but their scope of mitigation is now more limited. COBIT process DSS05.02 focuses on implementing network filtering mechanisms to control inbound and outbound traffic in accordance with policies.

The majority of the current data protection controls form part of the defense-in-depth strategy, but many of these controls have limitations when it comes to addressing the current threat landscape, resulting in unmitigated risk. Looking forward, additional solutions should be evaluated to further lessen the risk of unintentional data loss.

The Future of Data Protection

Ultimately, technical security controls should focus on protecting data. This means knowing and dynamically changing policy by controlling who is accessing sensitive data at the point of consumption and even when data leave the enterprise's boundaries. Organizations should build capabilities to analyze data usage inside and outside of their network to identify anomalies of access based on the role of an individual trying to access specific data. Additionally, data encryption should be decoupled from applications to leverage the scalability of the cloud and enable data protection at creation, in use, at rest and in transit. These steps will serve to bind security, access management and analytics to data.

Conclusion

The cost of noncompliance and loss of trust due to unintentional and intentional data loss are high; incidents are too frequent. Leaders in the organization must focus on developing a data protection strategy that provides the control, scalability, visibility and flexibility needed to meet the needs of the ever-changing threat and regulatory landscape. These security characteristics enable those empowered to mitigate risk to prevent, identify and mitigate unintentional data loss.

Endnotes

1 Alphabet Inc., 2016 10-K Form, 2017, *https://abc.xyz/investor/pdf/20161231_alphabet_10K.pdf*

2 Department of Health and Human Services (DHHS), "Enforcement Highlights," USA, 31 March 2017, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html*

3 European Union, "General Data Protection Regulation (GDPR) Portal: Site Overview," *www.eugdpr.org/eugdpr.org.html*

4 European Union, "GDPR Key Changes," *www.eugdpr.org/key-changes.html*

5 *Ibid*.

6 Department of Health and Human Services (HHS), "Top Five Issues in Investigated Cases Closed With Corrective Action, by Calendar Year," USA, 16 September 2016, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/top-five-issues-investigated-cases-closed-corrective-action-calendar-year/index.html*

7 Department of Health and Human Services, "Data Breach Results in $4.8 Million HIPAA Settlements," USA, 7 May 2014, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/new-york-and-Presbyterian-hospital/index.html*

8 California Correctional Health Care Services, "Potential Breach of Patient Health Information," USA, 13 May 2016, *www.cphcs.ca.gov/docs/press/Release%20-%20Potential%20Breach%20PHI.pdf*

9 Department of Health and Human Services, Office for Civil Rights, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," USA, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf*

10 Department of Health and Human Services, "Alaska DHSS Settles HIPAA Security Case for $1,700,000," USA, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/alaska-DHSS/index.html*

11 Department of Health and Human Services, "Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement," USA, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/catholic-health-care-services/index.html?language=es*

12 Smitheringale, S.; "New Report: Patient Confidentiality Broken 6 Times a Day," Big Brother Watch, 14 November 2014, *https://www.bigbrotherwatch.org.uk/2014/11/new-report-patient-confidentiality-broken-6-times-day/*

13 New Hampshire Office of the Attorney General, "Re: Notification of Data Security Incident," USA, 17 April 2014, *www.doj.nh.gov/consumer/security-breaches/documents/willis-north-america-20140417.pdf*

14 Department of Health and Human Services "HHS Settles With Health Plan in Photocopier Breach Case," USA, 7 August 2013, *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html*

15 Seward, Z. M.; "Bloomberg Accidentally Posted Private Terminal Messages Online," *Quartz*, 13 May 2013, *https://qz.com/84004/bloomberg-accidentally-posted-private-terminal-messages-online/*

16 Sanger, D. E.; N. Perlroth; "Bank Hackers Steal Millions via Malware," *The New York Times*, 14 February 2015, *https://www.nytimes.com/2015/02/15/world/bank-hackers-steal-millions-via-malware.html?_r=0*

17 ISACA, *COBIT® 5 Implementation—Supplemental Tools and Materials*, USA, 2 December 2013, *www.isaca.org/COBIT/Pages/COBIT-5-Implementation-product-page.aspx*

18 Harris, K.; "California Data Breach Report 2012-2015," California Department of Justice, February 2016, *https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf?*

19 Pugh, S.; Data Protection Update Course, The Proscenium, Atlanta, Georgia, USA, 22 September 2016