PART I

The Problem and Basic Tools

CHAPTER 1

The Problem: Securing Confidential Electronic Documents

The element of surprise has accounted for more victories throughout history than any other tactic, according to Sun Tzu in *The Art of War*. In 1941, the United States military was surprised by the attack on Pearl Harbor and, as a result, would learn a valuable lesson about preparedness and vulnerability.[1]

WikiLeaks: A Wake-Up Call

Today, attacks on organizations' information infrastructure occur daily, siphoning off confidential information. The most well-known cybersecurity breach is that associated with the WikiLeaks incident, in which confidential military, diplomatic, and corporate information was accessed and exposed online. This is perhaps the most visible example of an information security failure, but all types of organizations—not just the government and military—are at risk. And such breaches can be difficult to discover. Many times these types of incursions take place undetected for months, or even years, compromising the position of the victim organization and eroding the value of its information and stakeholder equity.

Since it is now widely known and accepted that the impact of leaked confidential information is real and the consequences are serious, organizations must constantly be on guard to protect confidential documents. There are specific steps that can be taken to counter the ongoing threat.

A number of countermeasure steps and processes that support information governance (IG) are available. These must be implemented alongside new technologies to enforce electronic document security (EDS). IG deals with the policies that control access to and use of information. They are a critical first step. For instance, in the case of WikiLeaks, a U.S. Army private

allegedly provided classified military information to Julian Assange. A policy should have been in place to disallow low-level personnel from accessing the Secret Internet Protocol Router Network (SIPRNet), which is used to transmit classified information. Protecting confidential e-documents begins with robust and thorough policy analysis, starting with the questions "How are we going to govern the use of our confidential information? Who gets access to which information? Where? And when?"

> Ironically, the technology that could have secured documents and prevented them from leaking is used by WikiLeaks itself to control access.

Once these key questions are answered, newer EDS technologies can be applied to enforce the policies and control the access and use of information. Commercial and defense software providers have created systems that can safeguard electronic documents and records, wherever they may reside or be transported. The latest generation of this technology has advanced so that policy management is more streamlined and control over e-documents can occur remotely, anytime or anyplace, whether on a hard drive, thumb drive, mobile device, website, or in transit.

The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents and records, from their creation and use to their final archiving or destruction.

In 2010, the federal government took steps to better protect its information infrastructure by launching United States Cyber Command (CYBERCOM). The mission of the project is to "synchronize the Defense Department's various networks and cyberspace operations to better defend them against the onslaught of cyber attacks."[2] Unfortunately, it does little to address the issue of misuse of authorized data retrievals by insiders with security clearance. That is where clear and enforced IG, and technology tools, are critical to securing internal information assets.

> The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents and records, from their creation and use to their final archiving or destruction.

This book details the specific policies that need to be created for various information delivery platforms as well as the specific technologies that are needed to control, manage, and audit the use of electronic documents. These solutions are available; they simply take time, a focused effort, an adequate budget, and strong management resources to accomplish. And IG is not a one-off, one-time effort; once the program is in place, it must be consistently monitored, audited, and reviewed. *Leaving an organization vulnerable to data spills and breaches is due to poor management, and presents an avoidable business risk.* This risk can be avoided with proper policy analysis, planning, communication, and auditing as part of an overall IG program, and by leveraging security technologies.

U.S. Government Attempts to Protect Intellectual Property

The theft of intellectual property (IP), which includes software source code, patented designs and blueprints, research, customer lists, and business methods, is a growing problem, and the U.S. government stepped in to combat it. In early 2010, the Department of Justice (DoJ) formed an IP task force to focus law enforcement efforts on the nettlesome and increasing problem of IP theft.[3]

The DoJ is trying to coordinate at multiple levels to streamline efforts between state, federal, and international law enforcement agencies to address IP theft, which has real economic consequences, especially for providers of software which is commonly illegally copied. Access to proprietary software source code must be securely monitored as it is a critical information asset for software development companies. The same is true of other providers of IP, such as law firms, consulting firms, advertising agencies, research companies, and the like.

Threats Persist across the Pond: U.K. Companies on Guard

The problem of inappropriate or criminal access of confidential information assets spans the globe. In the United Kingdom, it was reported that cases involving employees taking confidential data from the workplace tripled from 2008 to 2009, and they have continued to increase today.[4]

Hard economic times may have contributed to the rise, as employees moved to new jobs or started new businesses using confidential information (e.g., client contact information) stolen from their previous employer. But many of these cases could have been prevented with proper IG polices and enforcement using EDS technologies.

Increase in Corporate and Industrial Espionage

Corporate espionage is not new, and it has tangible costs. Ford is reported to have suffered a loss estimated at $50–$100 million as a result of the theft of confidential documents by one of its own employees. A former product engineer who had access to thousands of trade secret documents and designs sold them to a competing Chinese car manufacturer.

In another case of industrial espionage, the car manufacturer Renault filed a criminal complaint, asserting that another company tried to buy secrets related to its electric car program.[5] Several executives were ultimately suspended, showing that in our highly competitive business environment, ethics may be cast to the wayside if it means gaining an advantage—or, in the case of the complicit executives, financial gain. This can occur at the highest levels of enterprises, not just in the trenches.

Some schemes can be quite deceptive and devious, masked by standard operating procedures. Granting remote access to confidential information assets for key personnel is common. Granting medical leave is also common. But a deceptive and dishonest employee could feign a medical leave while downloading volumes of confidential information assets for a competitor—and that is exactly what happened at Accenture, a global consulting firm. During a fraudulent medical leave, an employee was allowed access to Accenture's Knowledge Exchange (KX), a detailed knowledge base containing previous proposals, expert reports, cost-estimating guidelines, and case studies. The employee went to work for a direct competitor and continued to download the confidential information from Accenture, estimated to be as many as 1,000 critical documents. While the online access to KX was secure, the use of the electronic documents could have been restricted even *after* the documents were downloaded, if newer technologies were deployed to secure them. Software security protections can be employed to seal the documents and control their use—even after they leave the organization.

> Ford's loss from stolen documents in a single case of IP theft was estimated at $50–$100 million.

Other recent high-profile industrial espionage and document leakage cases include:

- Hybrid car trade secrets were stolen from General Motors by an engineering employee in a scheme to sell them to rival Chinese car manufacturers.

- Huawei Technologies, the largest networking and mobile communications company in China, was sued by U.S.-based Motorola for allegedly conspiring to steal trade secrets through former Motorola employees.
- Health information of 1,600 cardiology patients at Texas Children's Hospital was compromised when a doctor's laptop was stolen. The information included personal and demographic information about the patients, including their names, dates of birth, diagnoses, and treatment histories.[6]
- Car burglars made off with personal records of 4,000 patients of a Portland, Oregon, psychologist and the names and Social Security numbers of 2,900 jobless residents in the county.
- MI6, the U.K. equivalent of the U.S. Central Intelligence Agency (CIA), learned that one of its agents in military intelligence attempted to sell confidential documents to the intelligence services of The Netherlands for £2 million GBP ($3 million USD).
- U.K. medics lost the personal records of nearly 12,000 National Health Service (NHS) patients in just eight months. Also, a hospital worker was suspended after it was discovered he had sent a file containing pay-slip details for *every* member of staff to his home e-mail account.[7]
- Personal information about more than 600 patients of the Fraser Health Authority in British Columbia, Canada, was stored on a laptop stolen from Burnaby General Hospital.

The list of breaches and espionage could go on and on, more than filling the pages of this book. It is clear that it is occurring and that it will continue. Safeguarding confidential information assets cannot rely solely on the trustworthiness of employees and basic security measures. It takes up-to-date information governance efforts and newer technology sets. Executives and senior management can no longer avoid the issue, as it is abundantly clear that the threat is real and the costs of taking such avoidable risks can be high. A single security breach can cost the entire business.

Risks of Medical Identity Theft

Rising medical identity theft is alarming and damaging to consumers and represents a liability for health care organizations. The U.S. government has become more involved, establishing the President's Task Force on Identity Theft and a medical-specific program in conjunction with the Office of the National Coordinator for Health Information Technology (ONC).[8] There are new initiatives and incentives for health care providers and institutions to automate health records. However, this move toward electronic patient records carries new medical identity theft risks. ONC commissioned

technology consulting firm Booz Allen Hamilton to conduct a study of the extent and impact of medical identity theft, the results of which were published in a January 2009 report. It stated, in part:

> *The consumer has the greatest potential for loss as well as key roles in prevention, detection, and remediation. Of course, many other parties may be involved or affected by medical identity theft. An individual may inappropriately access health data when it is held by many participants in the health care delivery chain, including the insurer, health care provider, a third party (e.g., lab, pharmacy), or the consumer. When these misappropriations result in medical identity theft, however, the impact on the consumer has the possibility of being the most severe.*
>
> Some potential effects on the consumer include compromise of patient care as a result of inaccurate health information entering his or her health record; inability to receive health insurance or other benefits; or financial obligations for services that were never received. *In turn, the consumer is most knowledgeable about his or her own health record and, therefore, is the first line of defense for protecting against medical identity theft and identifying a potential issue early, which may help to reduce the damage.* [emphasis added][9]

The consumer has the most to lose from medical identity theft.

Why Don't Organizations Safeguard Their Information Assets?

A leading document security software provider has issued this statement, which sums up the problematic irony in most organizations, regarding their internal documents:

> *Despite repeated examples of data loss the industry has witnessed over the past few years, and despite their disastrous consequences, many organizations still lack clear data security policies and fail to deploy the right security arsenal to prevent them. While they take all the necessary measures to protect their physical infrastructure and facilities—controlling and restricting access to their physical sites—they fail to protect their informational and digital assets. Yet, this is where a company's innermost secrets, intellectual property and value resides—confidential files, financial documentation, acquisition plans, customer information, sensitive e-mails, exclusive product releases and other corporate records. All are ultra-capital assets that need to be shielded from the outside world.*[10]

Organizations lacking in the policies and technologies necessary to protect their internal confidential documents and communications should begin an IG initiative and investigate technologies that can assist in enforcing policies, such as endpoint security tools like information rights management (IRM) that can secure electronic documents from their creation through their entire lifecycle.[11]

But it's not all about technology. It is also about leadership, communications, and corporate culture. Leveraging and enforcing IG policies to create a culture of security and compliance may be the best weapon senior management has to combat internal theft and industrial espionage. Communications and training must be planned, methodical, and regular. Safeguarding information assets is not a project—it is a constant process.

One thing is painfully true: Corporate espionage will continue to increase. Most of it will go undetected, quietly eroding information assets over time. The biggest question is whether or not your organization has put in place the necessary steps to counter it and mitigate its risk, or whether it will suffer steep losses like so many others.[12]

> The most effective way to prevent industrial espionage is by embedding data and document security into an organization's culture.

The Blame Game: Where Does Fault Lie When Information Is Leaked?

When information is spilled through an unintentional disclosure or data breach the most frequent scapegoat is the employee who was closest to it. He or she could be the person who lost a thumb drive or laptop, or the one responsible for securing a particular document type in their functional area. The higher-ups zero in on this person and place the blame squarely on them, but what level of responsibility does the employer share? Are they not responsible for corporate governance, and therefore IG? Are they not responsible for providing the technology and tools to help secure confidential information assets?

There are policies that must be formed and technologies that must be deployed, and these are the responsibility of the employer and senior management. In the event of a data breach, they need to *first* look at their IG policies and business processes. Were the procedures (and enabling technologies)—the tools employees need—in place to protect critical documents and data? Are lines of responsibility clear? Is there auditability and accountability?

Accidental or unintentional data breaches can be as damaging as malicious or intentional ones. So IG policies must be set and tested and audited regularly to ensure compliance and effectiveness. Only certain employees should have access to confidential information assets, and always at the proper time. Also, employees must be made aware of possible ways to lose or compromise data. Training should be ongoing. Communication should consistently enforce the message over a variety of media, week after week, month after month. As Peter Abatan states in his blog, "It is only after an organisation has employed the right tools that it can begin to hold its employees responsible for a security breach."[13]

Consequences of Not Employing E-Document Security

A senior executive pondered what could happen if his organization did not use EDS software for safeguarding critical documents. What are the potential consequences? The following are six ways an organization can be negatively impacted, according to Abatan:

1. *The perceived value of your business is eroded slowly through the loss of your intellectual property to competitors that former employees join or new startups by former employees.*
2. *Investor confidence in your business' ability to safeguard trade secrets begins to wane.*
3. *You really don't have full control of where your information assets are located and as such you cannot know when your confidential information gets into the wrong hands.*
4. *You cannot control how your confidential information or sensitive data is used once you send it to a third party.*
5. *Staff could mail confidential documents or sensitive data to the wrong recipient after which you have no control.*
6. *You might never know when your intellectual property is taken without permission and used in a way that is counter-intuitive to your business.*[14]

In addition, there is the potential direct cost of fines and legal fees for compliance failures.[15] To mitigate this risk, managers need to find out how technologies, such as IRM and data loss prevention (DLP)—which are discussed in detail later in this book—can prevent the flow of confidential information and intellectual property to competitors, and also develop and enforce IG to implement the policies needed to protect confidential e-documents.

Chapter Summary: Key Points

- Electronic document security (EDS) came to the forefront with the revelation of leaked documents openly published by WikiLeaks. This should be a wake-up call to all organizations.
- The goal of a program to secure confidential information assets is to provide complete document lifecycle security (DLS) for critical electronic documents.
- Industrial espionage and loss of confidential documents is rising, and will continue to increase.
- Loss of confidential documents and intellectual property causes real economic damage to organizations, and erodes information asset value.
- Organizations should first take a serious look at the business processes that support information governance when there is a data breach or loss/misuse of confidential information assets.
- Leakage and misuse of internal e-documents can be avoided by developing information governance strategies to create and enforce policies for EDS, and by deploying specific technologies to monitor compliance.

Notes

1. Bill Blake, "WikiLeaks, the Pearl Harbor of the 21st Century," *edocument Sciences, LLC*, posted December 6, 2010, http://edocumentsciences.com/wikileaks-the-pearl-harbor-of-the-21st-century, retrieved July 10, 2011.
2. Ibid.
3. Antone Gonsalves, "Justice Department Launches IP Task Force," *InformationWeek Government*, posted February 15, 2010, www.informationweek.com/news/government/policy/showArticle.jhtml?articleID=222900277, retrieved March 9, 2012.
4. James Hurley, "Companies Warned as Data Theft Disputes Surge," *The Telegraph*, posted November 24, 2010, www.telegraph.co.uk/finance/businessclub/8157244/Companies-warned-as-data-theft-disputes-surge.html, retrieved March 9, 2012.
5. Peter Abatan, "Corporate and Industrial Espionage to Rise in 2011," Enterprise Digital Rights Management, www.enterprisedrm.info/post/2742811887/corporate-espionage-to-rise-in-2011, retrieved March 9, 2012.

6. Todd Ackerman, "Laptop Theft Puts Texas Children's Patient Info at Risk," *Houston Chronicle*, July 30, 2009, http://www.chron.com/news/houston-texas/article/Laptop-theft-puts-Texas-Children-s-patient-info-1589473.php, retrieved March 2, 2012.
7. Jonny Greatrex, "Bungling West Midlands Medics Lose 12,000 Private Patient Records," *Sunday Mercury,* September 5, 2010, http://www.sundaymercury.net/news/sundaymercuryexclusives/2010/09/05/bungling-west-midlands-medics-lose-12-000-private-patient-records-66331-27203177, retrieved March 2, 2012.
8. U.S. Department of Health & Human Services, "ONC Commissioned Medical Identity Theft Assessment" http://healthit.hhs.gov/portal/server.pt?open=512&objID=1177&parentname=CommunityPage&parentid=12&mode=2&in_hi_userid=10732&cached=true, retrieved August 1, 2011.
9. Booz Allen Hamilton, "Medical Identity Theft Final Report," January 15, 2009, www.nachc.com/client/Medical%20Identity%20Theft%20Final%20Report-ONC.pdf.
10. Quoted in Robert Smallwood, "Securing Documents in the WikiLeaks Era," *KM World*, posted May 28, 2011, www.kmworld.com/Articles/Editorial/Feature/Securing-documents-in-the-WikiLeaks-era-75642.aspx, retrieved August 1, 2011.
11. Peter Abatan, "Corporate and Industrial Espionage to Rise in 2011," Enterprise Digital Rights Management, www.enterprisedrm.info/post/2742811887/corporate-espionage-to-rise-in-2011, retrieved March 9, 2012.
12. Ibid.
13. Peter Abatan, "Who Should Be Blamed for a Data Breach?" Enterprise Digital Rights Management, retrieved February 2, 2012.
14. Peter Abatan, "What Could Happen If You Don't Employ Enterprise Rights Management," Enterprise Digital Rights Management, www.enterprisedrm.info/, retrieved March 9, 2011.
15. Adi Ruppin, e-mail to the author on August 30, 2011.