Information Management

ROT or Not?

How a Records Retention Schedule Can Reduce the Garbage, Risks, and Costs

Tom Corey, Esq., CRM

Organizations are required to retain certain information, and the cost of failure can be high. But keeping ROT – redundant, outdated, and trivial information – can have even more costly consequences. Here is how a well-executed retention schedule can mitigate the risks and costs.

When an organization begins the painstaking process of identifying its records, organizing them into groups, and assigning retention policies to them, employees often ask why it's necessary. The answer can be organized around four simple words: space, compliance, discovery, and breach.

Space

Early records management was needed simply because space was an issue. File cabinets got so full that employees could no longer add or remove files, and additional files would end up on top of the cabinet and on the floor. Organizations had two options: 1) make space for more file cabinets or 2) get rid of records they did not need.

Onsite Storage

In many cases, the high cost of commercial real estate makes that decision easy. For example, *The Real Deal* reported $80 per square foot in Midtown Manhattan, New York, early last year, making the cost of adding a single commercial lateral file cabinet about $950 a year. In St. Louis, Missouri, it would cost $23.34 per square foot, or $250 annually, according to this year's *St. Louis Annual Market Report* from Gershman Commercial Real Estate.

Offsite Storage

Offsite storage facilities provide a less costly solution to storing files initially, but they generally have other costs to access, re-shelve, and destroy files. Another issue is that when records are located far away, they are not quickly available when needed, which decreases their value and could raise a question about how beneficial retaining them is.

Electronic Storage

Electronic storage may seem to resolve space issues, but not if it requires an onsite data center pod. According to Neil Rasmussen in *Calculating Space and Power Density Requirements for Data Centers*, a pod, which is a cluster of cabinets with power and a cooling infrastructure, requires up to 16 square feet of space. Using the per square foot calculations mentioned above, each IT cabinet would cost $5,100 per year in Manhattan and $1,500 in St. Louis.

Even information stored on portable devices, such as laptops, flash drives, and compact disks, has a space cost related to the equipment required to retrieve it.

Records that have value are worth the cost of the space; others are not. A retention schedule can be used to distinguish between those for which the cost of storage is justified and those that can be dispositioned to save the organization space and money.

Compliance

When U.S. President Franklin Roosevelt signed the Fair Labor Standards Act into law, in 1938, it established a 44-hour work week, 25 cents minimum wage, rules that required employers to retain records, and government authority to inspect the records. Today, the U.S. government requires organizations to retain a variety of other records as well (e.g., employment, customs, environmental, tax, and industry-specific), which it also has the right to inspect.

Civil Penalties

Perhaps the greatest fear organizations have is not about what is in their records, but about what required records they are missing. Their inability to produce required records for inspection quickly (or at all) can cost them a great deal of money. Following are several examples of potential fines that can be levied.

A retention schedule can be used to distinguish between those [files] for which the cost of storage is justified and those that can be dispositioned to save the organization space and money.

The U.S. Occupational Safety and Health Administration (OSHA) fined an Ohio Home Depot store more than $150,000 in 2013 for violations that included its inability to produce required records within a four-hour inspection window, according to an Aug. 26, 2013, OSHA news release.

Per "Clean Air Act Vehicle and Engine Enforcement Case Resolutions" on the U.S. Environmental Protection Agency (EPA) website, the EPA can fine an organization up to $45,268 per day for recordkeeping and reporting violations.

According to 19 U.S.C §1509(g), U.S. customs' agents can issue a fine up to $100,000 or 75% of the appraised value of merchandise for willful record violations and up to 40% of the appraised value of merchandise for negligent recordkeeping violations.

Criminal Penalties

The enactment of the Sarbanes-Oxley Act of 2001 (SOX) took potential recordkeeping penalties to a new level – from civil to criminal. The act was precipitated by the well-known downfall of Enron and accounting firm Arthur Andersen, who – while preparing for a U.S Securities and Exchange Commission investigation – began destroying paper and electronic records they were required to retain.

Under SOX, public accounting firms are required to maintain audit work papers and data to support filings for seven years (see 15 U.S.C. §7213(2)); public corporations must maintain accounting audit or review work papers for five years (see 18 U.S.C. §1520); and the public company must maintain and document a system of internal controls and procedures for financial reporting (see 17 C.F.R. § 229.308).

These provisions are enforced by requiring the company's chief executive officer and chief financial officer to sign the quarterly and annual reports certifying the accuracy of the information under penalty of law (ssee 17 CFR § 232.302 and 17 CFR § 240.14d-1). With the potential of criminal actions facing top executives of public companies for publishing inaccurate information, the push to maintain proper records became a corporate mission.

Discovery

For a short time, cheap electronic storage seemed to be the answer to space and compliance concerns. Organizations could choose to retain all their information forever electronically, so they would always have required records. This solution was short-lived.

A 2016 Veritas Global Databerg survey shows how pervasive the storage of unneeded information is. Its "Report Finds 85% of Stored Data is Either Dark, Redundant, or Trivial (ROT)" found that only 15% of an organization's stored data is business critical; the rest has either an unknown value or is considered ROT. (ROT also stands for redundant, outdated, and trivial.)

An often-cited but unverified statistic attributed to Gartner Research says professionals spend 50% of their time looking for information and take 18 minutes to locate each document. In the April 2013 *Harvard Business Review* article "Email Is Not Free," Tom Cochran wrote that a study he conducted in his company determined that each sent or received e-mail cost 95 cents for labor.

Time Is Money

E-discovery requires organizations to use legal professionals and sometimes software tools to collect, process, and review their electronically stored information (ESI) and distinguish between what information is relevant and irrelevant to the legal action. The greater the volume of information there is to review, the more expensive the process.

The key problems with retaining everything forever are the extraordinary length of time and amount of money spent searching for needed information …

The key problems with retaining everything forever are the extraordinary length of time and amount of money spent searching for needed information when the electronic storage repository is filled with a bunch of junk. Both increase exponentially when the search is to find all relevant information during e-discovery.

ROT vs. Not

Parallels can be drawn between an electronic repository and a closet. The more stuff jammed into a closet, the harder it is to find that winter scarf when it gets cold. Enlarging the closet or building another closet will not necessarily make it easier to find that scarf. A more efficient approach is to remove the things that are no longer needed – like the now-adult daughter's elementary school backpacks and the long-unused yoga mats.

In the same way, storage repositories are often full with both useful and useless things; for example, they may include not only the needed final documents, but many drafts for each final, and e-mail correspondence with companies that have not existed in years.

To make it more complicated to find what is needed, this information is often in employee-created folder systems on laptops and shared drives that are so creative and complex that when employees leave, the knowledge of how the information can be located also is gone.

Time is money, and too much time is spent going through information "closets" looking for information. Time is especially expensive when it is spent by lawyers reviewing potentially relevant ESI, including e-mails, instant messages, documents, databases, websites, and even metadata, for e-discovery.

And lawyers have been especially busy with e-discovery since 2004. That is the year of the landmark case *Zubulake v. UBS Warburg* and other cases that sanctioned parties for failing to preserve ESI they knew was relevant or ESI that could have reasonably been calculated to lead to the discovery of admissible evidence.

Trying to avoid sanctions, or spoliation, which can include fines, evidence rulings, or adverse jury instructions, can be extremely expensive. The 2012 Rand study "Where the Money Goes? Understanding Litigant Expenditures for Producing E-Discovery" found that the cost of review for e-discovery ranges from $20,000 to $40,000 per gigabyte. In the 2010 *Duke Law Journal* article "Defining the Problem of Cost in Federal Civil Litigation," the authors wrote that discovery costs typically consume 20-50% of total litigation costs.

The key way to reduce these costs is to get rid of the ROT, retaining only information that is useful to the organization, thereby reducing the volume of information that could be subject to e-discovery.

Breach

Hackers want private information because it may contain personally identifiable information (PII), such as Social Security numbers, credit card numbers, or health information. In too many cases, organizations retain private information long after it has value to the organization but still has value to hackers and can cause damage to the organization if breached.

Financial Impact

In most states, a breach of PII requires notification to those impacted by the breach. In California, which was the first state to enact this requirement, personal information is defined by Cal. Civ. Cd., §1798.92 as "a person's name, address, telephone number, driver's license number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, savings account number, or credit card number."

Ponemon Institute's "2016 Cost of Data Breach Study: United States" found the cost of each document stolen in a security breach is $221, and the total average cost to handle a data breach incident is $7 million. This calculation included direct costs, such as investment in technologies and legal fees, along with indirect costs, such as investigation time and management of breach notifications.

Other Consequences

Hackers sometimes go after more than PII and financial data. In 2014, a group calling itself the Guardians of Peace hacked Sony e-mail accounts containing private conversations among Sony executives. A *Los Angeles Times* headline revealed the financial damage: "Sony says studio hack cost it $15 million in fiscal third quarter." But the revealed e-mail conversations among Sony executives, producers, and others regarding celebrities and public officials caused embarrassment for the parties involved, a public relations nightmare for the company, and the firing of the head of Sony Pictures, Amy Pascal.

More recently, information from a hacked e-mail account played a role in last year's U.S. presidential election. In October, just before voting began, WikiLeaks began releasing private e-mails – some more than 15 years old – from the account of candidate Hillary Clinton's campaign chairman, John Podesta. Clinton has characterized WikiLeaks as one of the two "determinative" factors in her loss.

While both hacks were information security failures, they were also a failure of records management. It is unlikely that many of the old e-mails that were leaked had any value to Sony or Podesta, yet they had a great deal of value to those wishing to inflict damage with them.

Solutions

As organizations are becoming more aware of the costs and risks associated with the four information-related issues addressed in this article – space, compliance, discovery, and breach – and invest in technology and other resources to help address them, they can also minimize the threat and mitigate their costs and risks simply by disposing of information they no longer need. Implementing a quality information governance program, which includes a strong records retention component, is the principal way to accomplish this objective. E

About the Author: Tom Corey, Esq., CRM, is a manager within the information governance practice of HBR Consulting LLC, working with law departments to create, implement, and maintain information governance/records management policies, including reviewing compliance with domestic and international requirements. He earned his law degree from Charlotte School of Law, is a Certified Records Manager, and is an active member of the North Carolina State Bar, Mecklenburg County Bar, and the American Bar Association. Corey can be contacted at *tcorey@hbrconsulting.com*.