blancco
technology group

WHITE PAPER

The Information End Game

What You Need to Know to Protect Corporate Data Throughout its Lifecycle

INTRODUCTION

Your corporate data is crucial to your business success. But the more information you manage, the more risk your enterprise carries.

After Sony lost 100 terabytes of data to a cyber attack in November 2014 the company was criticized for lax records management. The most brand-damaging files included tens of thousands of emails that exposed the inner workings of Sony Pictures and controversial conversations between studio executives. Had unneeded emails regularly been **erased from the corporate servers**, the studio would have suffered far less exposure and damage.

Sony is hardly the only company to fall victim to a data breach. But its misfortune holds lessons for virtually every enterprise.

Most organizations hoard corporate data assuming that all information retains value over time or that it's cheaper and easier to keep data than to destroy it. But most data outlives its use quickly and in many industries only a small proportion of records need to be retained indefinitely. But once data is no longer valuable, it becomes a liability and can expose your organization to extreme costs and risks.

To mitigate the risk of data exposure and avoid the costs of storing and handling unnecessary information, organizations need end-to-end processes for managing information throughout its entire lifecycle. In particular, organizations need a carefully constructed plan for effectively destroying data when it reaches its end-of-life.

Data Downsides

The fact is that organizations are creating, storing and transmitting more information than ever before. In 2013, the global volume of data was 4.4 zettabytes (ZB). By 2020, that number will balloon to 44 ZB – the equivalent of 44 trillion gigabytes.[1]

While corporate information holds tremendous value, it also carries inherent risks. The more data you have, the more likely it is that sensitive information can be exposed.

Such information includes:

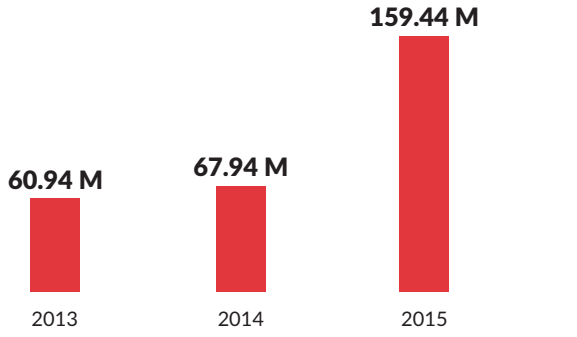
Customer Data: This involves personally identifiable information (PII) that could identify a specific person such as name, address, account numbers, financial data and Social Security numbers. It also covers protected health information (PHI), such as medical records or associated payment data.

Employee Data: This includes the same details as PII, plus information such as salary and performance reviews.

Corporate Data: This includes intellectual property, such as trade secrets, research and development data, as well as marketing plans. It also covers other sensitive information, such as customer lists, financial results and internal communications. Increasingly, it might include Internet of Things (IoT) data from manufacturing, supply chains and other operations.

But as organizations manage more information data theft continues to occur. This is evident in the growing number of data breach news headlines that come out each day. Cyber attacks exposed nearly 160 million data records in 2015 — a huge jump over previous years.[2] (See Figure 1.) These attacks are increasingly carried out by sophisticated, well-financed players, such as organized crime groups and rogue governments. And they target organizations of all sizes and across all sectors, including private and public entities.

1 "The Digital Universe of Opportunities," IDC, April 2014
2 Privacy Rights Clearinghouse data, January 2016



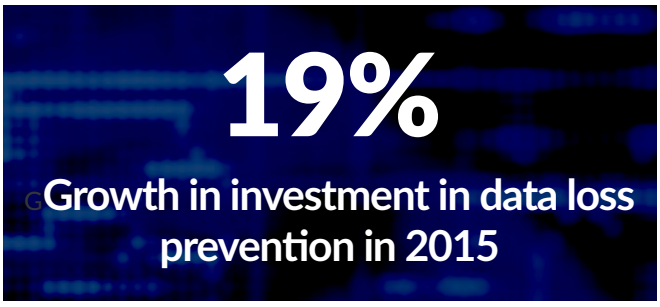
Source: Privacy Rights Clearinghouse

The number of publicly reported exposed data records has risen dramatically.

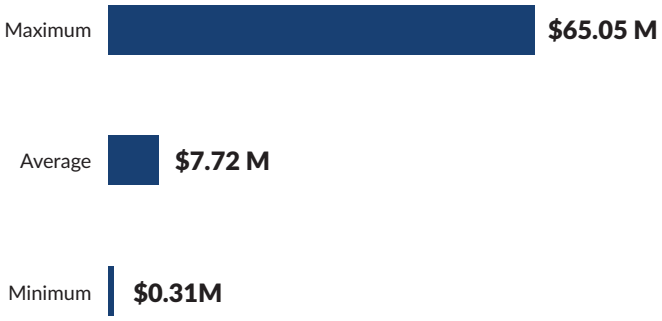
Figure 1: Data Breaches

But data breaches aren't the only concern. Managing more data also exposes your organization to audits and legal risks. Any time your organization goes through an audit and any time it's involved in legal action, your data may be subject to review and e-discovery. The more unnecessary data you have, the greater the unnecessary exposure for your organization.

What's more, data involves costs. First is the expense of protecting information from cyber attacks. More data on more servers, storage equipment, backup tapes and mobile devices means more places and ways you need to invest in cybersecurity. Worldwide spending on information security exceeded $77 billion in 2015, a year-over-year jump of 8 percent. The area clocking the fastest growth is data loss prevention, at 19 percent.[3]



Second is the cost of a data breach. Exposure of information comes with a hefty price tag – for everything from investigating the incident to remediating the problem to communicating with affected parties. In fact, the total one-year cost of a cyber crime incident ranges from $308,000 to as high as $65 million, with an average cost of $7.7 million.[4] (See Figure 2.)



Source: "2015 Cost of Cybercrime Study," Ponemon, October 2015

The average total cost of a cybercrime incident is $7.7 million.

Figure 2:Cybercrime Costs

But there are other less measurable, yet equally tangible costs associated with retaining data beyond its end-of-life. One is the cost of procuring and maintaining data storage and backup equipment. Another is the cost of maintaining personnel, processes and software to manage short-term data storage, near-term onsite backup and long-term offsite data archiving.

Just as significant is the productivity cost for every knowledge worker who must sift through unnecessary data to find needed information. If each of your employees spends even 30 extra seconds a day finding the information he or she needs, the productivity cost can easily add up to hundreds of thousands or even millions of dollars a year.

Data Management from Cradle to Grave

The costs and risks of retaining unnecessary data place a premium on managing data from the time it's created until it's erased at end-of-life. In fact, effective information management requires a data lifecycle strategy that involves six distinct phases. (See Figure 3.) Your mission-critical information needs to be protected at each of these phases.

3 "Forecast: Information Security Worldwide, 2012-2018, 2Q14 Update," Gartner, August 2014
4 "2015 Cost of Cyber Crime Study," Ponemon, October 2015

Effective information management calls for a life-cycle approach, from data creation through end-of-life.

Figure 3: Information Management Life Cycle

Create: Data creation involves the generation of new digital content or the updating or modifying of existing content. Creation can take place on-premise either in your data center or on your employees' devices, or it can take place externally in the cloud. Most corporate data is generated by business functions such as finance, human resources, marketing and sales, as opposed to the IT department, which is typically responsible for managing data *after* it has been created.

Data protection during the 'Create' phase includes access control such as passwords, threat scanning such as antivirus software and data classification that specifies the type of data, where it's located, who has access to it and how it should be protected.

Store: Data storage is the act of saving digital information in a repository, such as a computer hard drive or a data center storage device. Storage typically takes place at or shortly after creation, though certain types of transaction or analytics data might be generated in transit or in memory but not permanently stored to disk. Storage also involves near-term backups that must also remain protected. Once data is stored responsibility for its management typically falls to the IT or security team.

Storage protections include access control around who can read and overwrite the data, device control such as data encryption, backups to protect the data from loss, plus security measures to protect the backups themselves.

Use: During usage, data is accessed, viewed or processed. While data may be altered as it's being used, data modification is more accurately thought of as part of the 'Create' phase. Responsibility for protections during use falls equally on the lines of business and the IT department.

Protections during data usage include access control, encryption, data rights management for copyrighted information and data loss prevention, which involves software and business rules to prevent unauthorized access to sensitive information.

Share: Data often must be shared among users either inside or outside the enterprise. Sharing can take place over a network, across the Internet or through the exchange of removable media, such as thumb drives. When data is in transit, it's subject to a new set of risks.

Data sharing safeguards involve access control, encryption, digital rights management and data loss prevention. They also include network security, such as firewalls and intrusion detection and prevention.

Archive: For near-term protection, data must be backed up regularly, either onsite or offsite. But when data needs to be retained for the long term, it's archived – typically to tape media and usually in remote, secure locations. Data archiving trades easy availability for the lower cost and greater security of offsite storage.

Archiving is often the domain of the operations team as opposed to IT or the lines of business. Protections during this phase include access control and encryption.

Destroy: When data reaches end-of-life, it should never languish in an unused, unclassified state. Instead, it must be permanently erased. Determining which data is erased, how it's erased and how that erasure is verified depends on several factors, such as content type, usage needs and regulatory requirements.

When it's considered at all, the 'Destroy' phase is most often addressed by the operations team. But when managed properly, end-of-life data destruction is truly the responsibility of all stakeholders, from IT to the lines of business.

Gone, But Not Forgotten

Many organizations mistakenly assume they can manage data at end-of-life by simply deleting it. But usual file deletion commands don't actually erase data. Instead, they merely remove pointers to the disk sectors where the data resides. Such "deleted" data still remains stored on the disk. And that **data can easily be recovered** with readily available software tools.

Most CIOs and IT pros are aware of this fact. But many people in the lines of business are just waking up to the idea that data they assume was deleted is, in fact, vulnerable to exposure.

To truly protect your customer information, employee records and intellectual property, your organization needs comprehensive, certified data erasure. Certified data erasure can be achieved only through **enterprise-class software** that truly erases and verifies the erasure of sensitive information.

Effective data erasure also requires a lifecycle mindset that aligns data erasure with your business needs. Such an approach enables you to strategize, budget, target, standardize and **report** on your enterprise data erasure.

As spending to prevent data loss increases, it's important to consider how much of that investment should address data erasure. One way to approach the question is to track what you spend to secure data during its lifetime. That includes spending on access control, antivirus software, firewalls, device control, as well as development of the policies and procedures to implement those measures.

The fact of the matter is that data erasure only represents a small fraction of that overall expenditure. (See Figure 4.) Yet it's an investment many otherwise secure organizations fail to make.

Who's Responsible for Your Data?

Which department owns the information in your organization?

The IT team is thinking about data security. The legal department considers data from the perspective of risk management. The lines of business just want to know they can create, store, use and share information whenever they need to. Data end-of-life, if it's thought of at all, is typically the purview of the operations team.

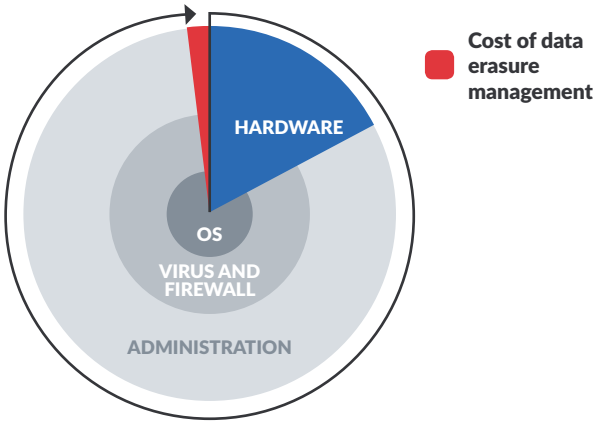
But in many enterprises, no one is thinking about overall information lifecycle management. And that can lead to gaps that expose your organization to serious security risks and costs.

What's required is a collaborative approach that involves all stakeholders. Ideally, that begins with sponsorship at the executive level. Depending on the value of data to their business success, some enterprises are even establishing a Chief Data Officer (CDO). You then need an information governance team that involves the lines of business, legal, IT and operations teams.

To the extent the lines of business depend on data, they can't just assume someone else is managing it. They should reach out to the legal department to make sure they're in compliance with relevant regulations. And they should actively engage with IT to ensure the right policies, tools and processes have been put in place to protect mission-critical information.

IT needs to extend protections for data throughout its entire lifecycle, including end-of-life. As part of that effort, IT should work with the lines of business so that they understand the requirements and challenges of data protection.

It's quite possible the policies and procedures that govern information lifecycle management will end up residing in IT. But all stakeholders must be actively involved to ensure that data remains protected from the moment it's created until it's destroyed at end-of-life.



The investment to achieve effective data erasure represents only a small fraction of the overall costs for enterprise data security.

Figure 4: Data Erasure Investment

From Regulation to Policy

Information lifecycle management, including the destruction of data at end-of-life, begins with data protection policy. Ownership, or at least sponsorship, of that policy, begins in the executive suite. Some organizations even establish a Chief Data Officer (CDO) to ensure data protection is prioritized. (See Sidebar: "Who's Responsible for Your Data?")

Depending on your corporate structure, your data protection policy should involve IT, Security, Legal, Risk Management and the lines of business. At the highest level, your policy should specify the following:

- How data is classified
- How long each type of data will be retained
- How data will be protected at each phase of the information lifecycle
- How it will be destroyed at end-of-life
- Roles and responsibilities for relevant stakeholders

Of course, how you classify data and how long you retain each type of data isn't entirely up to you. In the face of data breaches, data protection regulations have proliferated.

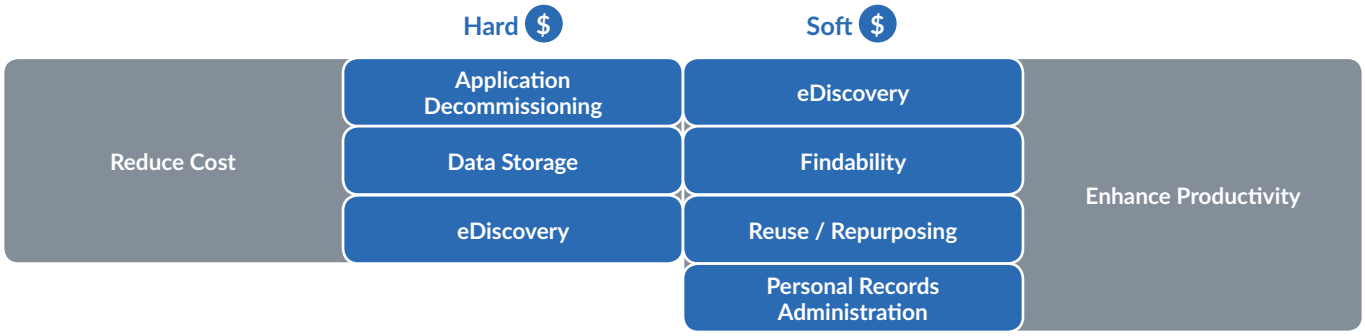
At least 75 countries have data protection laws, as do U.S. states such as California and Massachusetts. Organizations must now comply with both general and industry specific regulations and guidelines, from Sarbanes-Oxley information security standards to the Health Insurance Portability and Accountability Act (HIPAA) to the Payment Card Industry Data Security Standard (PCI DSS).

More regulations are on the way. The Obama Administration's Consumer Privacy Bill of Rights, proposed in 2015 would require industries to establish codes of conduct around data and create privacy boards overseen by the U.S. Federal Trade Commission (FTC). Also in 2015, the European Union (EU) overhauled its 1995 Data Protection Directive. The new regulation, which goes into effect in 2018, will strengthen citizen rights such as the "right to be forgotten," or erased from data records. The rules apply to companies with services that process EU citizen data even if the servers are located outside the EU.

In many countries, data protection laws specify how long records must be retained. For example, under Sarbanes-Oxley, some records must be kept for four years and some indefinitely. Under HIPAA, some records must stay on file for seven years and some permanently. PCI DSS requires a documented data retention policy and the purging of unnecessary data on a quarterly basis. It also defines the scope of an audit as all data that's "relevant" — so the fewer unnecessary records you retain, the fewer will be subject to audit.

The risks and costs of ignoring data protection throughout the information lifecycle are clear. So are the benefits of prioritizing information lifecycle management, from data creation through data destruction. (See Figure 5.)

Organizations that fail to effectively safeguard information face the expense and legal exposure of regulatory non-compliance, data breaches, damaged reputation, lost customers and more. But strategic organizations that invest the necessary efforts and resources in information lifecycle management can minimize the costs and risks of their mission-critical information, from data creation through its safe and verifiable destruction when it reaches end-of-life.



Benefits of effective information lifecycle management include lower costs, reduced risk, and improve productivity.

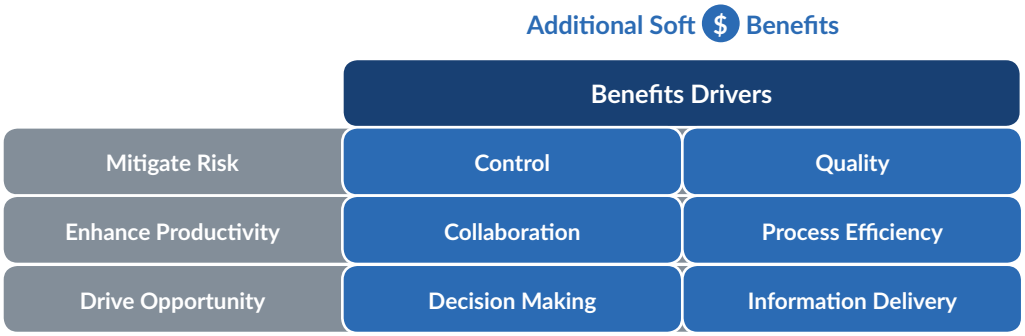


Figure 5: Financial Impact of Information Lifecycle Management

Source: Deloitte

ABOUT BLANCCO TECHNOLOGY GROUP

Blancco Technology Group is a leading, global provider of mobile device diagnostics and secure data erasure solutions. We help our clients' customers test, diagnose, repair and repurpose IT devices with the most proven and certified software. Our clientele consists of equipment manufacturers, mobile network operators, retailers, financial institutions, healthcare providers and government organizations worldwide. The company is headquartered in Alpharetta, GA, United States, with a distributed workforce and customer base across the globe.

Blancco, a division of Blancco Technology Group, is the global de facto standard in certified data erasure. We provide thousands of organizations with an absolute line of defense against costly security breaches, as well as verification of regulatory compliance through a 100% tamper-proof audit trail.

SmartChk, a division of Blancco Technology Group, is a global innovator in mobile asset diagnostics and business intelligence. We partner with our customers to improve their customers' experience by providing seamless solutions to test, diagnose and repair mobile assets. SmartChk provides world-class support, pre and post implementation, allowing our customers to derive measurable business results.

CONTACT US

For Sales & Marketing, Please Contact:
Email: marketing@blancco.com

For Corporate Communications & PR, Please Contact:
Email: press@blanccotechgroup.com