Not if, But When You Get Hacked

Measuring and Proactively Managing Information Risk

By Russell Stalters, CEO Clear Path Solutions Inc.

If this is true, then what are organizations to do? These increased cyber security threats corporations face today is a big concern for Board members and CEOs. The Chief Information Security Officer (CISO) along with help from the Chief Privacy Officer, General Counsel (GC), and CIO are tasked with keeping the company safe and addressing this risk.

Organizations should have an effective Information Governance (IG) strategy that aligns with their overall enterprise risk management strategy and that can be effectively operationalized to leverage and protect information assets while accomplishing broader business goals and reducing the organization's overall risk profile.

A challenge faced by many organizations is the lack of a meaningful information risk assessment process. This is especially true when determining a way to measure the efficacy of the IG Program. This paper discusses steps to assess these information risks with the goal of creating an Information Governance Scorecard and provides recommendations for establishing proactive monitoring of these risks as a vital first step to reduce the organization's risk profile.

Over the years, **Russell Stalters**, CEO of Clear Path Solutions Inc. and author of gettinginformationdone.com has established a reputation as a subject matter expert for information governance, information and data management, SharePoint and Office 365 based solutions. Most notably until 2016, as Director Information & Data Management for BP's Gulf Coast Restoration Organization, he was responsible for the information architecture, data management strategy and geographic information services. In that role he served as the Chief Architect with full design authority for all business applications and data management solutions created to manage approximately 1 petabyte of information and data collected during the response and restoration efforts from the Deepwater Horizon Incident and Oil Spill.

Also while at BP serving on the Enterprise Architecture Team, he was Global Head, Information Architecture responsible for BP's information architecture and information management standards. Mr. Stalters joined BP as Global Director, Information & Records Management leading global operations and heading up BP's Data Privacy & Protection program.

He also helps organizations innovate, transform, and maximize the effectiveness of individuals by helping them improve their ability to lead, work together, select and develop their people. He has honed these skills as a certified member of the John Maxwell Team and is personally mentored by John C. Maxwell.

A regular industry speaker, noted author, and thought leader, he presents at national and international industry conferences. In 2014 he was inducted into the Association of Imaging and Information Management (AIIM.org) Company of Fellows to recognize him as an expert in the field of information management. Russell has a master's degree in Computer Science from the University of Florida and is a retired Naval Officer and Naval Aviator.

Contents

Information Risk Contribution to Enterprise Risk

Most organizations think of data breaches or cyber-attacks when they think of information related risks. These are just one of many risks that companies must consider when addressing the contribution of information risk to overall enterprise risk. Typically, companies respond by focusing their resources on the latest threat until another information related risk pops up – almost like a game of whack-a-mole. Proactive and regular risk assessment can eliminate this phenomenon and enable organizations to prioritize their risk reduction resources more effectively.

Information risks that contribute to enterprise risk include:

- Inability to respond to regulatory requirements completely and consistently
- eDiscovery-related risks such as noncustodial data sources missed in legal hold execution, resulting in potentially relevant information inadvertently modified or deleted, or material issues of dispute that are poorly understood until well after the strategy is established and expenses incurred, along with excessive redundant, obsolete, trivial (ROT) data, causing litigation costs to exceed value of dispute.
- Excessive ROT data contributes to potential personally identifiable information (PII) data breach exposure.
- Sensitive data leaks including intellectual property (IP) and PII can result in reputational risk, fines, and other costs.
- Business decisions made on missing or poor quality information, resulting in ineffective or faulty conclusions can increase safety and operational risks.
- Data maintained in IT systems which is poorly understood can lead to incomplete or incorrect application of retention, disposition, preservation, privacy, and collection policies.
- Poor understanding of data held in legacy systems prevents IT from appropriate data disposal and decommissioning of systems causing significant and unnecessary costs with the associated risk.

Without a robust Information Governance Program and an effective way to measure its effectiveness, organizations can be exposed to significant information risks which contribute to overall enterprise risk. The following describes these risks and the impact they can have on an organization.

Protection of Intellectual Property and Sensitive Corporate Data

Much of the information that has real business utility within an organization includes intellectual property and other sensitive corporate data. Knowing where this information is stored and ensuring appropriate controls are in place protects this information against internal security violations or external security breaches. Without adequate security and effective controls in place there is potential for this data to leak from the organization which can expose the organization’s unique capabilities and secrets to a competitor and increase Enterprise risk. In some cases, this data may benefit from being stored encrypted. But the first order of business is to make sure that all intellectual property and sensitive data is identified throughout the organization.

Legal Hold and eDiscovery Processes

These two Legal processes can contribute significant risk to Enterprise Risk. The first is an effective Legal Hold compliance risk and the second is predominately a financial risk related to the eDiscovery and litigation support process.

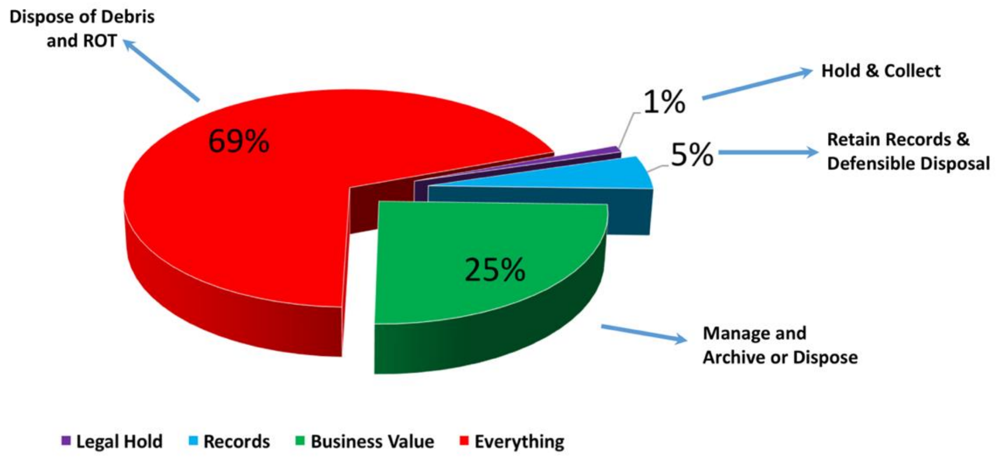
Focusing on non-custodial data subject to a Legal Hold, if the organization does not completely understand where data is stored within their repositories, either rogue or IT managed data sources can be missed during the legal hold execution resulting in potentially relevant information being inadvertently modified or deleted. Another Information Governance process risk is the inability to readily assemble, understand, or defend the preservation and discovery record. This can be a significant risk.

These are principally financial risks but the unneeded or incomplete documents and data can also lead to legal risks.

> *"It would be helpful if systems were in place to get rid of the junk. Part of the reason eDiscovery is so expensive is because companies have so much data that serves no business need... Companies are going to realize that it's important to get their information governance under control to get rid of the data that has no business need... in ways that will improve the company's bottom line."*
>
> The Honorable Andrew J. Peck,
> United States Magistrate Judge

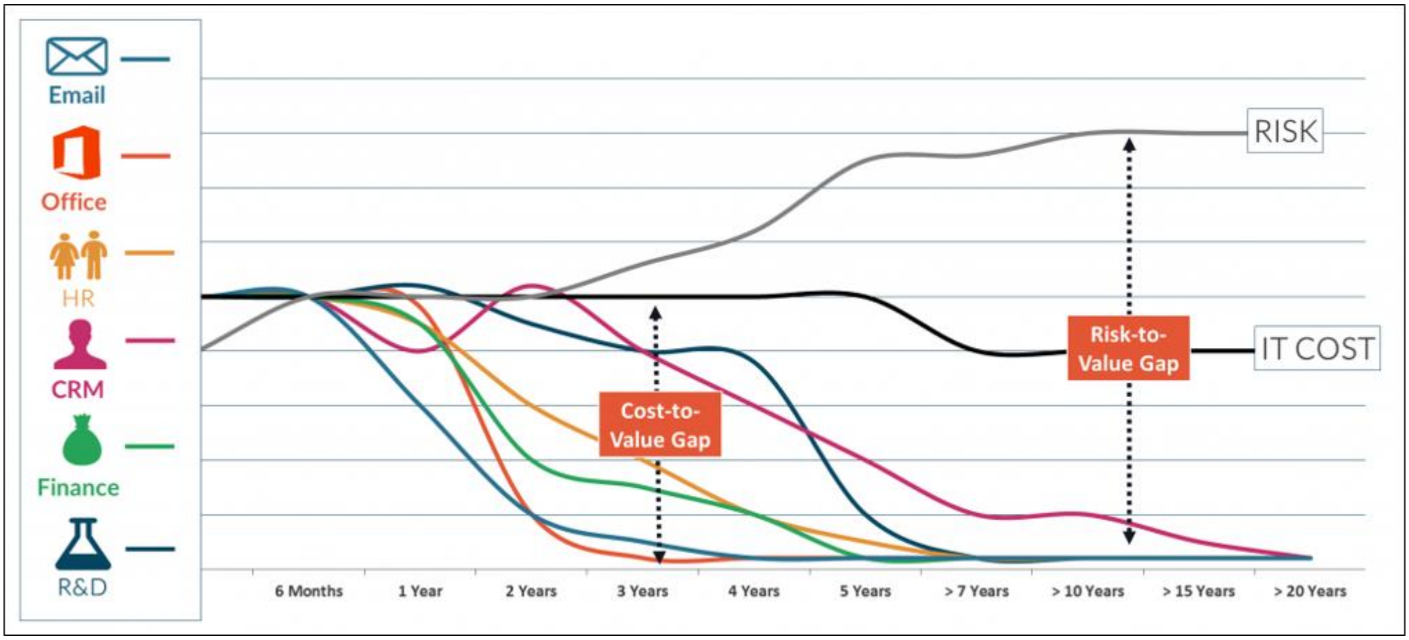
Information Quality

From the "Information Lifecycle Governance Leader Reference Guide" by Compliance, Governance and Oversight Council (CGOC), 2014 and from an earlier survey conducted: *"only 1% of enterprise information is subject to legal hold, 5% is related to regulatory record keeping, and 25% has real business utility. So what about the remaining 69% of the information deluge?"*



By eliminating unnecessary ROT data or digital debris as it has been called, business users will gain optimum value from corporate information assets. Additionally, organizations will be able to maintain tighter controls over costs and reduce overall exposure to information related risks. Quality is improved.

As the cost of storage decreased in recent years, IT has slipped into a 'save everything' mentality which increases the discoverable corpus of information, complexity, and legal risk. On the flip side, if IT disposes of information indiscriminately of business value, then enterprise operations are undermined. Preventing what can become a digital landfill is important because as most corporate data ages, its value dramatically decreases while risk due to litigation exposure and for a potential breach can increase.



Source: Information Economics: Understanding and getting value from your unstructured data, IBM Corporation 2014

Another related risk is important business decisions can be made on missing or poor quality information, resulting in ineffective decisions or potentially impacting operations or safety. Sometimes "missing information" occurs when the business has forgotten the source or location of information and can't find it, resulting in additional cost without corresponding value.

Data Breaches and Privacy Compliance

Cyber security is a strategic priority for most organizations. With the recent high profile breach incidents including Home Depot, Target, and Sony, many companies are asking themselves "Will I be next?". The answer is yes based on the number of widespread attacks daily. Although a high priority, the Chief Information Security Officer (CISO) has a limited budget to defend the organization.

The mindset that should be taken is "when we get hacked" not "if we get hacked".

Ultimately, the CISO needs to understand the information footprint across information systems, determine the value/risk of loss, and protect them against cyber-attacks through the deployment of control activities that are commensurate with the value/risk of these information systems. By doing this, digital security investments can be prioritized to provide different levels of protection to reduce the risk of losing sensitive data. In addition to sensitive business information, specific categories of information that need to be protected include:

- **Personally identifiable information (PII):** Information that can be used to identify, contact, or locate a single person, or to identify an individual in context. The EU has even broader definitions of PII.
- **Sensitive personal information (SPI):** e.g. data such as race, ethnicity, and political and religious opinions.
- **Protected health information (PHI):** Regulated by HIPAA, PHI includes any information related to an individual's health, condition, and treatment.

Failure to comply with these and other evolving regulations can impact the business including fines, prison terms, and reputational damage.

Proliferation of Information Systems and Repositories

Many companies are still trying to remediate the large number of file share repositories (Z, S, or G drives) which contain hundreds of terabytes of uncategorized and sometimes unknown content. eDiscovery Directors mention this as one of the leading risks they want to get after. They see the fact that much of this content is ROT and that most organizations have little idea what is actually contained in these repositories as a big litigation and compliance risk. These unknown pockets of information increase the chances of incompletely collecting, reviewing and producing responsive documents in compliance with eDiscovery orders.

Besides these repositories, many organizations maintain obsolete legacy information systems which contain potentially relevant information subject to eDiscovery and in most cases, information which should have been disposed of long ago.

The Value of Addressing These Information Risks

An effective information Governance Program coupled with a way to measure the magnitude of these risks can help an organization understand the contribution to overall Enterprise Risk and to prioritize investments to reduce these risks. The following sections describe the benefits of addressing the information risks discussed above.

Reducing the Costs Associated with eDiscovery

Costs associates with eDiscovery include collection, processing, and review. Using the definitions from the Electronic Discovery Reference Model:

- Collection costs are principally related to gathering electronically stored information (ESI) for further use in the eDiscovery process.
- Processing costs are related to reducing the volume of ESI and converting it, if necessary, to forms more suitable for review, analysis, and other tasks.
- Review is evaluating ESI to identify responsive documents for production and privileged documents to withhold.

The magnitude of these costs are directly correlated to the volume of the data that is collected, processed and reviewed. A study conducted by the RAND Institute for Civil Justice entitled: *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, 2012 found that costs for collection ranged from $125 to $6,700 per Gigabyte, from $600 to $6,000 per Gigabyte for processing, and from $1,800 to $210,000 per Gigabyte for review. At the low end this adds up to $2,500 per Gigabyte for collection, processing, and review.

Another article by MODUS, an eDiscovery services company in 2014, cited these costs at just over $500 per Gigabyte for processing and review, but does not include collection. To look at it from a dollars and cents perspective, the actual cost associated with processing and hosting of data has dropped more than tenfold. But, due to the increase in potentially responsive documents, **attorneys are required to review more than 10 times the amount of documents than before**.

Identifying and Reducing ROT

By reducing ROT and eliminating “digital debris”, organizations can realize real benefits and reduce the risk associated with this pernicious problem. Immediate benefits include:

- Improvement of information quality by removing redundant information made up of previous versions of documents, numerous drafts, most of which have no value once the final version is published.
- Reduction of the eDiscovery footprint which reduces the costs associated with collection, review and production.
- Potential for decommissioning of obsolete or underutilized storage and information systems. Annual cost savings estimated at $40K per IT application is conservative for most industries.

Reduce Impact and Chances of a Data Breach

By understanding the types of sensitive data and where it is located an organization can ensure that PII, SPI, PHI is identified and protected appropriately. In some cases, this data continues to be stored when it is no longer needed or located in unauthorized repositories like an employee laptop. Reducing the sensitive data stored in an organization allow the CISO to focus their protection resources on a smaller footprint. For instance, this known corpus of sensitive data can be encrypted to ensure protection even in the event the data is breached.

To appreciate the potential impact of sensitive data breach, consider the following as reported by Naked Security, "In total, the breach has cost Target $290M so far, of which insurance should cover $90M, the company said last week. However, there are still shareholder lawsuits to come, as well as probes by the Federal Trade Commission and state attorneys general, which could well push the total costs of the incident to over $300M." This is just one high profile case.

From the "2015 Cost of Data Breach Study: Global Analysis" conducted by Ponemon Institute LLC: *The cost of data breaches due to malicious or criminal attacks increased from an average of $159 in last year's study to $170 per record. Last year, these attacks represented 42 percent of root causes of a data breach and this increased to 47 percent of root causes in this year's study.*

This does not include the consequences of lost business which averaged $1.57 million or the losses that can be attributed to reputational consequences of a data breach.

The other benefit of addressing and improving the protection of sensitive personal data is compliance with global data privacy regulations. For example, in the UK the Information Commissioner's Office issues monetary penalty notices, requiring organizations to pay up to £500,000 ($650,000) for serious breaches of the Data Protection Act.

The following summarizes Information Risks and the value of addressing these risks.

Information Risk	Type of Enterprise Risk	Value of Addressing Risk
Improper Handling of Sensitive Data/IP	Financial, Business, and Legal	Avoid loss of business and potential litigation to recover compromised data.
Poor Legal Hold Effectiveness	Legal and potentially Financial	Improved preservation and compliance with Federal Rules of Civil Procedure, amended, December 1, 2015.
Increased eDiscovery Costs	Legal and Financial	Using $510+ to $2,500 per Gigabyte and a volume of 1 Terabyte, a 25% reduction in the data to collect, process, and review results in a $130K to $640K savings.
Poor Information Quality	Operation, Safety, and Business	Improved decision quality and operational consistency.
Excessive ROT	Financial, Operations, and Legal	Reduced storage costs and potential savings of $40K/year on decommissioned applications.
Data Breach of PII	Financial, Business, and Reputational	Avoid estimated cost of $170/record, potential fines, and lost business. The US average number of records for a breach was 28,000 in 2015 which equates to a cost of $4.76M.

Getting There – Reducing Enterprise Risk Through Effective Information Governance

Information Governance is not a project or one information management discipline. It enables the information management functions to be managed holistically as a Program. With an effective Information Governance Program, the organization can better understand and address enterprise information risks and their contribution to overall Enterprise Risk.

There are many resources available to support creating or revitalizing an Information Governance Program including:

> *"Information governance is the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs."*
>
> The Information Governance Initiative, http://iginitiative.com, accessed July 30, 2016

- The Information Governance Initiative: http://iginitiative.com
- Information Governance Reference Model (IGRM): http://edrm.net/projects/igrm
- CGOC (Compliance, Governance and Oversight Council): http://cgoc.com

The purpose of this white paper is not duplicate what is available at these sites and elsewhere.

Assuming the organization is committed to establishing or revitalizing the Information Governance Program, how can senior management and the Board know the magnitude of problem and the impact on the organization's enterprise risk profile? Information Risk needs to be measured.

Measuring and Proactively Managing Information Risk

To date, Information Governance maturity models have focused on subjective methods to assess the effectiveness of IG Programs. Examples include, ARMA International's Information Governance Maturity Model which is based on their Generally Accepted Recordkeeping Principles®, and the CGOC developed the Information Governance Maturity Model which defines the processes necessary for a robust governance system that crosses the primary set of stakeholders.

Organizations can use one of the maturity models listed above to conduct a subjective assessment of their Program as one of the inputs to an **Information Risk Scorecard**. The drawback by only using subjective measures is that the amount of risk is hard to quantify and prioritizing resource investments are difficult.

A better, integrated approach includes both subjective measures as well as objective methods to quantify and understand the magnitude of information risk which provides a more accurate picture of overall Enterprise Information Risk. By using a file analysis product like **Active Navigation,** organizations can understand their enterprise data footprint, both physically and geographically, as well as identify potential risks and the business value of the underlying data.

> *"File analysis enables storage managers, legal and security professionals, and business analysts to understand and manage unstructured data stores to reduce costs and risk, increase efficiency of business-critical data, and make better information management decisions for unstructured data."*
>
> Gartner Market Guide for File Analysis Software, August 4th 2015. G00271713

Conducting this type of enterprise-wide analysis creates a comprehensive data map by analyzing electronic files in place to create an efficient index for use in a wide range of information governance scenarios from content clean-up and disposal, through compliance and migration, to continual content governance. Benefits of creating a data map include:

- Profile the data estate to understand what you hold and design and act on policies driven by what data you actually have.
- Locate, remediate, and adequately protect files containing sensitive information.
- Identify the millions of ROT files, which once removed defensibly improve search quality and reduce risk.
- Design information protection strategies based on the business value or associated risk of the information.
- Helps the CISO prioritize investments for protecting sensitive information.

The **Information Risk Scorecard** is then made up of the subjective assessments of the IG Program based on a maturity model and the objective data collected during the creation of a data map. Together these two measures paint a more realistic picture which includes the magnitude of the information risk and helps identify areas to focus on which will deliver the largest reduction in risk.

Finally, it does no good to conduct the information analysis and create a data map one time. For the IG Program to be effective and for information risk to managed successfully, this assessment must be conducted regularly. With consistent policies in place, Active Navigation provides repeatable file analysis and monitoring becomes deliberate, managed and defensible rather than one-time or ad-hoc. Effectiveness of the Program is improved by:

- Policy violations are notified to responsible staff.
- Exception workflows are initiated for review, action and disposal.
- Reporting, review and disposal works at scale for efficient handling of large data estates.
- Helps prevent ROT from creeping back into the data estate.
- Provides periodic updates to the Information Risk Scorecard

Conclusion

In this world of increased cyber threats and likelihood that the organization will have some type of data breach in the future, the CEO, CISO, GC, Chief Privacy Officer and CIO working together, must look for ways to address these risks. An effective Information Governance Program is critical and foundational to managing the information risk contribution to overall Enterprise Risk. As Peter Drucker (writer, professor, management consultant and self-described "social ecologist") wrote: "What gets measured gets managed.". Unless there is a sound way to measure Program effectiveness those charged with managing these risks are only guessing.

File analysis adds precision to measuring the effectiveness of Information Governance by enabling clients to understand their data estate, create data maps and to understand the distribution of sensitive and PII information and ROT across that estate. Therefore, is it obvious that you should adapt this approach including the use of quantitative metrics, scorecards, along with solutions like Active Navigation to address these information risks.

About Active Navigation

Active Navigation is a recognized industry leader providing unique file analysis software for the discovery, transformation and ongoing control of unstructured data wherever it lies in the enterprise.

Its products play a fundamental role in any information governance strategy enabling cost, risk and efficiency savings through information audit, clean up and defensible deletion, intelligent file migration, records capture, eDiscovery collection and ongoing policy monitoring. Its globally proven methodology is driven by 10s of thousands of hours of practical experience and empowers information, IT and legal professionals to truly understand and take control of their unstructured data.

Active Navigation has a history of early innovation and leadership in file analysis and information governance, achieving Gartner Cool Vendor status and various Microsoft platform certifications as well as being a founding member of the Information Governance Initiative.

www.activenavigation.com