RICOH
imagine. change.

Understanding your information risk

5 steps to conducting a content risk assessment

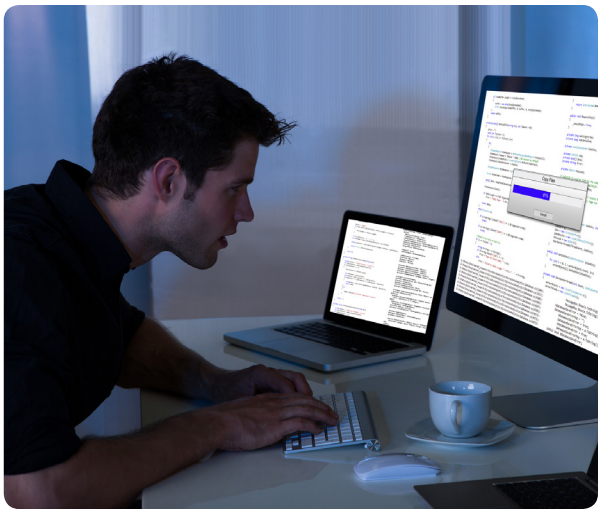
By David Gaffaney,
Ricoh Global Technology Advisor
April 2017

In one media report after another, high-profile companies have suffered through intellectual property leaks, employee and customer information breaches, and watched their reputations erode on social media—in some cases, along with their stock prices.

From the government and healthcare organizations to Fortune 500 companies and small businesses, no one is exempt from threats of a security breach. More than 554 million data records were lost or stolen in the first half of 2016, a dramatic increase of 31% compared with the previous six months, research shows.[1]

Hacking of the government's U.S. Office of Personnel Management exposed 21.5 million people to the theft of a vast trove of personal information including Social Security numbers and fingerprints.[2] Data breaches in healthcare totaled over 112 million records In 2015.[3]

Many organizations now realize they have little insight into their level of risk in this area and are reactively trying to understand where their data resides and how to control it. *After* a breach is the wrong time to find out. At the forefront of these concerns is the vast amount of unstructured content in file shares, ECM systems and email. Risk and exposure levels are often complete unknowns.



Hacking of the government's U.S. Office of Personnel Management breach exposed 21.5 million people to the theft of a vast trove of personal information, including Social Security numbers and some fingerprints.

Source: Jim Sciutto. CNN. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/

We don't know what we don't know

What information poses the greatest risk? This is a murky issue. Even for areas of known risk, such as email, there is often no consistent plan to address the exposure. To make matters worse, in today's world of information explosion, new data is created, shared and stored daily—both on premise and in the cloud.

Methods for storing this information are often unmanaged and inconsistent. The challenge lies not only in enforcing compliance with policies for content storage and usage, but in running a discovery or audit. Often, the information's true resting place is very difficult to track and determine. For example, data might be stored in unmanaged systems, like network shares, laptops or consumer storage like Dropbox or Google Docs. This lack of transparency makes companies uncertain about their next moves.

Combine the unstructured content with the chaos created by the accelerating growth of information, and it quickly becomes apparent that a manual inventory is simply not feasible.

[1] Gemalto 2016 Breach Level Index. http://breachlevelindex.com/assets/Breach-Level-Index-Report-H12016.pdf (Removed Group IT Governance Ltd stat)
[2] Jim Sciutto. CNN. http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million/
[3] Dan Munro. New York Times. https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#119f1b2b7b07

The purpose of a content risk assessment

The key to conquering content risk is having consistent, structured methods to identify, valuate and prioritize areas of risk. It starts with a content risk assessment. Using the results of a content risk assessment, you are able to:

- Define a mitigation plan for critical risk areas.
- Develop a governance model for sustainable management of unstructured information.
- Conduct periodic analyses across high-volume enterprise repositories.

Done properly, a content risk assessment can help you proactively plan for new or emerging media types, use proven methods that account for future growth, and help ensure new sources do not corrupt systems or expose the enterprise.

The end result is knowledge and understanding of your risk, a plan to manage critical areas and overall, more clarity around information-driven processes across key business areas. Transparency is key.

Strong data security is not optional

- U.S. data breaches increased 40 percent in 2016.
- For the eighth consecutive year, hacking/skimming/phishing attacks were the leading cause of data breach incidents, accounting for 55.5 percent of the overall number of breaches.
- Exposure of social security numbers was evidenced in 52 percent of the overall breaches in 2016.
- Exposure of records involving credit/debit cards was 13.1 percent.

Source: ITRC Data Breach Report 2016 by Identify Theft Resource Center and CyberScout. http://www.idtheftcenter.org/2016databreaches.html

5 steps to conducting a risk assessment

Taking on an information risk assessment is not quick or easy, but the sooner it's done, the sooner it will help protect your essential information assets.

1. Uncover critical risk and exposure

In some cases, this will be obvious. In highly regulated industries, the risk is well known for information such as clinical trial records in life sciences, customer account records in banking and patient records for healthcare. The key is to uncover other areas where high-risk information is also exposed. For example, a high-tech manufacturer's engineers may be working on research offsite and accessing information from USB drives or non-corporate-controlled hardware. These are your critical targets. Low-exposure, low-risk items will be the last things addressed. Here is a general guide:

Competitively sensitive information such as Intellectual Property; Regulated content under HIPAA, GLBA or other Federal/State mandates; Protected personal information such as PCI, PII, PHI. Managed in a repository with good security controls and appropriate access management. **No immediate action required, validate security assumptions and assure alignment with overall corporate strategy.**	Competitively sensitive information such as Intellectual Property; Regulated content under HIPAA, GLBA or other Federal/State mandates; Protected personal information such as PCI, PII, PHI. Managed in a repository with inadequate security controls and access management. Limited audit capability and traceability. **Immediate action required; Investigate movement to managed repositories with appropriate security and access controls.**
Non-competitive information, non-regulatory and less sensitive information. Maintained on a secure internal network. **No immediate action required. Align with overall corporate strategy.**	Non-competitive,non-regulatory and less sensitive information. Maintained on shared drives or externally sourced networks with fewer automated controls or security. **Move to managed technology with automated controls and in alignment with corporate security strategy.**

Level of Risk / Sensitivity

Level of Exposure

5 steps to conducting a risk assessment

2. Ask risk-based questions

It is important to be objective about risk and exposure. Ask questions about your content, such as:

- Does it contain *personally identifiable information* (such as PCI/PII/PHI)?
- Is it HIPAA-related? That includes medical records, certainly, but also pharmacy, employee wellness, disability and more.
- Is it commonly retrieved for audits (FDA, SEC, FERC, OSHA)? Which agencies regulate you?
- Does the content qualify as intellectual property? Engineering drawings, formulas, client/customer lists and critical processes must be in controlled repositories, not on USB sticks that are easily lost.

You can derive good exposure metrics from these questions:

- Is the content in a managed (structured) system or on a shared drive, a laptop, in consumer cloud services (like Dropbox or Google Docs) or personal email?
- Have roles been properly and clearly defined with regard to accessing certain types of content? Can your systems apply roles effectively?
- Do you understand the security as it applies to producer and consumer roles?
- Are process controls built into the creation, approval and distribution of content?
- What is the at-rest and in-transit encryption strategy for the content?
- Are there physical security controls in place, as applicable? This applies to paper, other non-digital assets, or servers, laptops, tablets and mobile devices.

Behind the evaluation above, there will be layers of considerations beneath the core factors that influence your scoring, such as on premise versus cloud, and application of proper records management methods.

Security threats are evolving

New ways of stealing data or infecting networks are evolving nonstop, such as accessing mobile devices, public clouds cloud infrastructures. In addition, user behavior is always a weak link the security chain. How damaging are the latest threats? Research shows:

- 75 percent of organizations surveyed were affected by adware infections.
- Nearly a quarter who suffered an attack lost business opportunities. Four in 10 said the losses are substantial.
- Nearly 30 percent lost revenue.

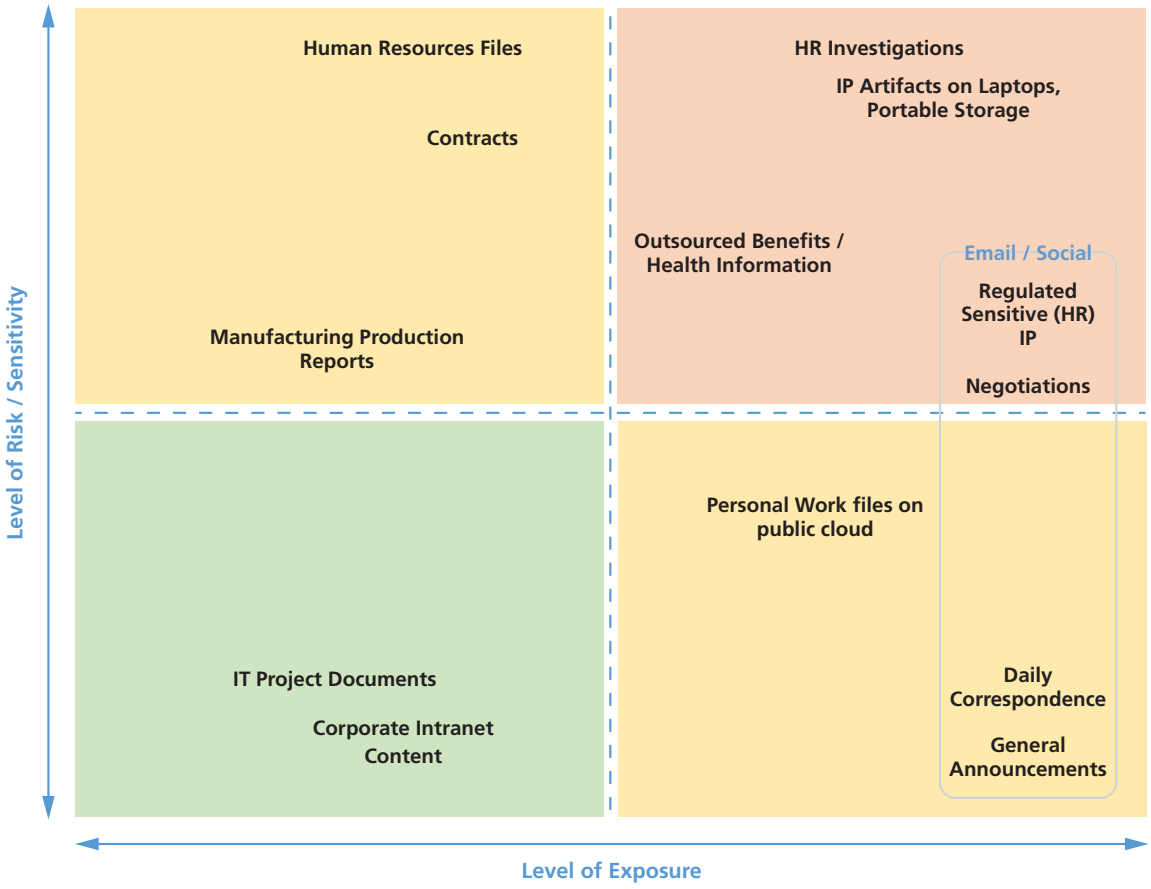
Source: Cisco 2017 Annual Cybersecurity Report. http://www.cisco.com/c/dam/m/digital/1198689/Cisco_2017_ACR_PDF.pdf

5 steps to conducting a risk assessment

3. Build evaluation results into a quadrant heat map

A heat map can function as a dashboard to show your current state and allow you to monitor your progress.

A sample assessment may look like this:



4. Prioritize areas of highest risk

Once this map is built, you will have a clearer vision of high-risk areas. Use the assessment to develop a roadmap of high-priority activities. Based on the example above, some key action items on the roadmap would be:

- Evaluate the management and encryption strategy for HR investigation records. This sample client stores these documents on shared drives, which triggers the exposure factor. Address the root cause.
- Confront challenges created by the movement of corporate IP. Our sample company is concerned about engineering drawings being stored on personal laptops and potentially on thumb drives, outside of corporate network control. A policy update is required.
- Address sensitive corporate records in email. The solution here may be to enact policies to store these records in a managed system as opposed to email. The solution could also involve a technology update or acquisition of an email archive application. Further investigation is required, but it is a high priority.

And so on. Each type of information will have its own action plan which, in combination with others, will uncover common patterns and identify methods for addressing issues.

5 steps to conducting a risk assessment

5. Tie strategy to business results

This methodology provides an initial point-in-time assessment that is extremely valuable for getting started. The value increases dramatically when paired with a quantified, prioritized roadmap.

With your enterprise content risk assessment in place, you are well positioned to address the high-risk areas, because now you are in charge of your critical information assets.

Equally important, the content risk assessment can help you sustain funding and progress for medium-risk content – a task that is nearly impossible without a quantified, prioritized roadmap. With your content risk analysis, you have the data necessary to build a fact-based strategic roadmap. For maximum impact, make sure your roadmap ties the strategy to business results.

Need help getting started?

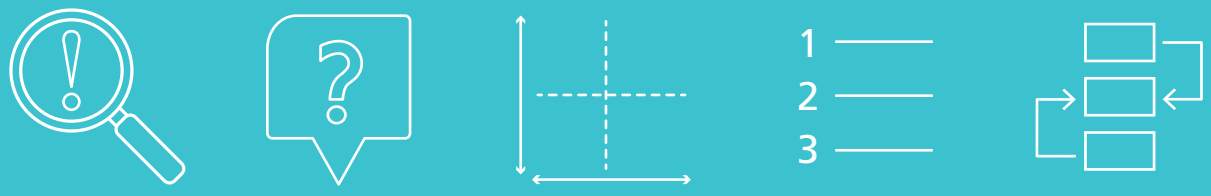
Want more information on content and risk assessments? Need help getting started on your strategic roadmap? Speak to your Ricoh specialist or visit www.ricoh-usa.com.

Spending on security: From prevention to detection

- Enterprises are shifting their security spending strategy in 2017, moving away from prevention-only approaches to focus on detection and response.
- Conventional security efforts and products have traditionally focused on blocking and prevention techniques (such as antivirus) as well as on policy-based controls (such as firewalls) to block threats.
- Worldwide spending on information security is expected to reach $90 billion in 2017, an increase of 7.6 percent over 2016, and to top $113 billion by 2020.
- Spending on enhancing detection and response capabilities is expected to be a key priority for security buyers through 2020.

Source: Gartner Research. http://www.gartner.com/newsroom/id/3638017

5 steps to conducting a content risk assessment



1. Uncover critical risk and exposure
2. Ask risk-based questions
3. Build evaluation results into a quadrant heat map
4. Prioritize areas of highest risk
5. Tie strategy to business results

RICOH imagine. change.

www.ricoh-usa.com

Ricoh USA, Inc. 70 Valley Stream Parkway, Malvern PA 19355 I 1-800-63-RICOH