



JATHEON
DATA | KNOWLEDGE | INSIGHT

Case Study



HOW TO AVOID THE HIGH COSTS OF NON-COMPLIANCE:

Stay Compliant with Email Archiving



TABLE OF CONTENTS

INTRODUCTION	3
NOT BEING AWARE OF REGULATIONS IS NOT AN EXCUSE FOR NON-COMPLIANCE	4
WHAT IS MORE EXPENSIVE, AN EMAIL ARCHIVING SOLUTION OR A LAWSUIT?	4
NON-COMPLIANCE IS MORE COMMON THAN WE MIGHT THINK	6
REGULATIONS EXIST AND WE CAN'T IGNORE THEM	6
WHAT IS AN EMAIL ARCHIVE?	7
WHAT DO YOU NEED TO DO?	7
COMPLIANCE BY ARCHIVING - STEP BY STEP	8
<i>ABOUT JATHEON</i>	10



INTRODUCTION

AT ONE POINT OR ANOTHER IN THEIR TRAJECTORY, MOST COMPANIES MUST FACE THE QUESTION OF WHICH IS HIGHER, THE COST OF COMPLIANCE OR THAT OF NON-COMPLIANCE. YOU WOULD BE SURPRISED HOW MANY ORGANIZATIONS OPT FOR NON-COMPLIANCE, PARTICULARLY WHEN IT COMES TO DATA SECURITY, FOR THE SAKE OF AVOIDING THE COSTS OF ESTABLISHING AN EMAIL ARCHIVE. THIS IS IN GREAT PART DUE TO A LACK OF AWARENESS OF ALL THE RULES AND REGULATIONS AND A BELIEF THAT IMPLEMENTING ARCHIVING IS MORE COSTLY AND TIME CONSUMING THAN IT REALLY IS.



NOT BEING AWARE OF REGULATIONS IS NOT AN EXCUSE FOR NON-COMPLIANCE

Most companies know that they are obliged to store sensitive information in one way or another, but, at the same time, many of them don't know what data is considered sensitive or in what way or for how long it needs to be stored. When you aren't sure what you need to do, you usually don't do it. Unfortunately, that doesn't make for a valid excuse in court. If your company gets sued for, say, breaching data privacy regulations, saying "I wasn't familiar with the rules" won't let you off.

Although decision makers and managers avoid archiving due to the costs associated with it, they should consider the substantial cost they are likely to face as a result of non-compliance.

Strangely, even companies which are aware of their responsibilities when it comes to data protection and archiving under compliance legislation don't always implement archiving solutions, simply because they want to avoid the costs. Although decision makers and managers avoid archiving due to the costs associated with it, they should consider the substantial cost they are likely to face as a result of non-compliance.

WHAT IS MORE EXPENSIVE, AN EMAIL ARCHIVING SOLUTION OR A LAWSUIT?

How high can the costs of non-compliance be, you might ask. Let's talk numbers.

- **\$5.6 million class-action lawsuit**

In 2015, Peterborough Regional Health Centre just outside Toronto, Canada faced a \$5.6 million class-action lawsuit alleging breach of privacy. The hospital admitted that 280 patient files had been wrongfully accessed, with seven employees fired as a result.



If staff had been aware of data compliance laws and if the hospital had had an appropriate information management system, this situation could have been avoided.

- **Political costs**

In 2013, Ontario's Information and Privacy Commissioner launched a special investigation into allegations that political staff in the former Canadian Minister of Energy's Office



inappropriately deleted emails pertaining to the sensitive subject of the cancellation and relocation of gas plants. The Commissioner found the staff at the Office had broken the law and had routinely deleted emails in an effort to avoid transparency and accountability, with two chiefs of staff being held directly responsible for the deletion of the emails.

This sparked political debate in local media as opposition parties looked to discredit those associated with the scandal. In addition to the potential cost of re-training current and hiring new staff and reviewing record retention policies, the political cost of this incident was undoubtedly significant.

- **Loss of reputation**

In 2010, a member of staff from Woodwinds Hospital, St Paul, Minneapolis, removed 200 copies of confidential patient files and kept them at her home for months without the hospital being aware of what had happened. The event resulted in a lawsuit between the staff member in question and the hospital.

Apart from the lawsuit, the hospital also suffered a damaged reputation. Given the extremely sensitive nature of the information they handle, health organizations (and companies from many industries) are under intense scrutiny when it comes to data security. A data security breach can seriously tarnish an organization's reputation.

In this particular case, Woodwinds Hospital could have avoided the entire incident by making sure they handled health information in compliance with the appropriate regulations.



NON-COMPLIANCE IS MORE COMMON THAN WE MIGHT THINK

Numerous companies and organizations lose thousands and even millions of dollars putting out fires caused by their lack of compliance.

These are just some of the cases that illustrate the high costs of non-compliance with the appropriate data retention rules and regulations. Numerous companies and organizations lose thousands and even millions of dollars putting out fires caused by their lack of compliance, not to mention the loss of reputation, time, and peace of mind they inevitably face in such situations.

Organizations can prevent troubles like these by simply implementing an archiving solution that ensures compliance with all of the necessary rules and regulations.

REGULATIONS EXIST AND WE CAN'T IGNORE THEM

It is as simple as this - emails and other types of digital communication are considered important records which must be retained and produced at a regulator's request. Every industry has its own retention period, that is, the duration of time for which records should be securely stored. While email archiving is the basic requirement across most industries, other types of communication data, such as instant messages, also need to be archived.



WHAT IS AN EMAIL ARCHIVE?

An email archive is a system that automatically obtains messages, attachments, and information about the messages from email servers, and then indexes and stores the information in read-only format for a specified period of time, depending on the particular retention policy.

Why is it not enough to simply back up data, as most companies and organizations already do? Archiving is necessary because most regulations require the retention of emails and other forms of communication in a read-only format, including their metadata (date of creation, last modification, etc.), for a certain period of time. Additionally, companies are not only required to store internal communication, but also need to be able to produce it when needed, ready for eDiscovery.

WHAT DO YOU NEED TO DO?

By not implementing an archiving solution in times of intense regulatory scrutiny, companies ignore the writing on the wall. Organizations of all sizes from industries all over the spectrum face the need to comply with extensive rules and regulations regarding the retention of emails, instant messages and social media information. Those who fail to comply are increasingly at risk of audits, government investigations and lawsuits, and can face fines or even, in severe cases, imprisonment, as dictated by regulatory bodies.

By not implementing an archiving solution in times of intense regulatory scrutiny, companies ignore the writing on the wall.

Such costs are greater than those associated with implementing an archiving solution. And while the implementation of such archives might seem like an ordeal, it does not have to be one at all. There is a series of steps you can follow to lead your company from a perpetual risk of fines to complete regulatory compliance - take a look at the checklist below.



COMPLIANCE BY ARCHIVING - STEP BY STEP

1. Identify your problems

Most companies have more than one problem that can be solved with email archiving. Make sure you understand all your needs before purchasing archiving technology so that you can choose the archiving solution that is a right fit for you.

2. Pick a solution that complies with all of your regulatory requirements

Once you have identified the regulatory requirements which apply to you, find an email archiving solution that meets them all. A comprehensive archiving solution will help you stay on top of your game when it comes to compliance and will save you many headaches and hours wondering whether you've done everything you should.

3. Create a data retention policy

An effective retention policy should address what the policy covers, as well as your company's data retention guidelines, procedures and responsibilities. It should also include retention timeframes for all the different types of data you want to retain and retention schedules that everyone will be able to follow and remember easily.

4. Inform all employees

Make sure you inform all your coworkers of the new or existing policy clearly and adequately and make sure it is easily accessible by everyone. All employees should be properly trained and made aware of all the legal and regulatory requirements and possible consequences of non-compliance.



5. Use both archiving and backups

Both email archiving and backups are essential for data security. Do not exclude your archives from backup and disaster recovery plans. A combination of on-premises email archiving and off-premises backup storage is usually a solid plan that makes Disaster Recovery (DR) a lot more manageable.

Many companies and organizations avoid implementing the appropriate archiving systems simply because they want to avoid the costs associated with them. By doing so, they actually put themselves at risk of suffering the much greater costs of non-compliance. These can range from thousand-dollar fines to million-dollar lawsuits, but can also lead to, perhaps even more dangerously, a damaged reputation and image or political costs.

Implementing an email archiving solution is a straightforward way of achieving complete regulatory compliance, which helps safeguard the company from the consequences of ignoring the regulations, and is certainly less pricey and less stressful than a run-in with the law.

Implementing an email archiving solution is a straightforward way of achieving complete regulatory compliance.

Find out how Jatheon can help you implement an archiving solution to achieve complete compliance by [contacting us](#) or by **requesting a demo**.



ABOUT JATHEON

Founded in 2004, Jatheon Technologies Inc. designed the world's first non-intrusive network appliance.

*Today, Jatheon continues to raise the bar throughout the industry with its latest enterprise grade **cCore** appliance line, and **ergo**, its powerful email archiving, indexing, retrieval and dynamic monitoring software solution, and best-in-class technical support, **The Jatheon Guarantee**.*

Jatheon is headquartered in Toronto, Canada and serves clients worldwide through its network of global business partners. For more information, please visit www.jatheon.com.