ENCRYPTION IS HOT APPLICATION IS NOT
Understanding the Cryptic Issue of Insufficient Use

WHITEPAPER
Author: Nicholas Sawarna
## CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>3</td>
</tr>
<tr>
<td>Survey Findings</td>
<td></td>
</tr>
<tr>
<td>Encryption Adoption</td>
<td>4</td>
</tr>
<tr>
<td>Implementation</td>
<td>5</td>
</tr>
<tr>
<td>The Case for Encryption</td>
<td>6</td>
</tr>
<tr>
<td>Our Lack of Disclosure</td>
<td>7</td>
</tr>
<tr>
<td>Handling Personal Data</td>
<td>8</td>
</tr>
<tr>
<td>Methodology</td>
<td>10</td>
</tr>
<tr>
<td>About Echoworx</td>
<td>11</td>
</tr>
</tbody>
</table>
As our reliance on the digital space continues to grow, so does our level of comfort with it. You might even say we are making ourselves right at home online. But, unlike our real world, where there are walls, drawers and safes in which to store our more valuable information, the digital world is uncomfortably exposed. And our reluctance to acknowledge how vulnerable we are online is risky when it comes to protecting privacy.

In a recent survey of IT professionals and IT decision-makers, conducted by Echoworx, key takeaways unanimously indicated encryption of information as a clear priority. But this priority appears to be only skin-deep – as less than half the organizations who have the software use it extensively. Considering how much personal information we provide online to a whole motley crew of banks, healthcare professionals and government bodies, this is alarming information.

In tandem with this survey, a separate survey was conducted on the contrast of how consumers divulge information online with their openness with prospective partners on first dates. When blended together, the two surveys suggest a striking communicational disconnect between the reasons why organizational decision makers value encryption and the actual frontline application of said privacy technology.
Encryption Adoption Continues to Grow

Encryption continues to grow steadily and is showing no sign of slowing down – with 53 per cent of the IT professionals and decision-makers surveyed identifying encryption technology as very important or even critical to their organizations. In addition to highlighting the importance of encryption, three quarters of these organizations indicate that they currently have encryption strategies in-place – a clear signal that encryption software is in their pipeline.

But this optimistic growth of encryption neither permeates through the organizations themselves, nor appears to be prioritized for the right reasons. When asked whether encryption technology is actually being used by their organizations, only 40 per cent of respondents said their organizations are using data privacy technology extensively. To further muddy the waters, a further 50 per cent of respondents admitted that they advocate for encryption to meet privacy regulations and avoid expensive breaches – not necessarily because they are concerned about protecting your private data.
Implementation Is Not Strong

A third of the average daily emails sent by IT workers which should be encrypted go out open and exposed in clear text. And, while encryption is available at these organizations, 62 per cent of them put the priority solely on external communications. This lack of implementation is alarming when you consider that many companies are now moving their email servers to the cloud – making even internal communications external in nature.

If enough data is leaked, an organization might be subject to a class action lawsuit, irrefutably damaging brand image.
The Case for Encryption Exists

Though nearly three quarters of people know what encryption means and why it exists, 45 per cent of them continue to send personal details through open email in a reckless manner. Thirty seconds or less, for example, is how much time people take to evaluate the safety of an email asking for personal information before sending their most-valuable information away – a statistic nearly as prominent for the safety evaluation of an online form.

The result? A considerable 24 per cent of people have had their information stolen.
Our Lack of Disclosure is Nothing New

Survey respondents show a lack of disclosure when it comes to sharing quantitative personal data to potential partners on a first date. These valuable pieces of information varied in terms of value on the black market, but displayed our willingness to let slip data about ourselves to complete strangers. Over a quarter of survey respondents, for example, are likely to share their real birth date, email address, full name and phone number on a first date – more than enough data to impersonate someone.

This lack of disclosure comes even more prominent when the survey group is broken out by sex – with men being the more reckless with their personal data. Predictable statistical results for men, for example, like the 12 per cent who choose to disclose their salary on a first date, are curiously identical to those same numbers of men who would provide their SIN card number online.

This behaviour directly translates online, with a whopping 49 per cent of men who have sent personal information by email they later regret. This same trend holds true for other digital activities, like applying for mortgage or online shopping.
Mishandling Personal Data is Expensive

When people trust you with their information, they are making you a liable party in the instance it is lost or stolen. With the new General Data Protection Regulation (GDPR), which effects all business in Europe and with European companies, for example, initial fines for breaching personal user data start at €20M.

And the expenses of a breach do not stop there.

In addition to massive fines for non-compliancy, there is the question of whether the issue is escalated further to brand-damaging class action lawsuits. Take Target's 2013 breach, for example, where various class action lawsuits, brand damage and initial fines have cost the company an estimated $240M to-date – a number which continues to grow.
Proactive Handling of Data Starts with Flexible Encryption

Despite there being a demand for encryption, the technology is not being used to its full potential within organizations offering it. One primary reason for insufficient use stems from the time-consuming difficulty of using older encryption software – both for front- and back-end users.

The solution?

Investing in a contemporary encryption platform package is the best way to encourage members of your organization to use it – especially for mobile. In addition to being faster and easier to use, newer encryption software integrates with ease with existing IT systems and offer multiple methods of protecting information in transit.

Here’s what to consider when choosing a high-performing encryption solution:

A. INFINITELY SCALABLE
Cloud, On-Premise or both

B. OFFERS SMOOTH USER EXPERIENCE
Provides a range of secure delivery options

C. EASILY INTEGRATES WITH EXISTING SOLUTIONS
Interoperability across desktop and mobile

D. SEAMLESS AUTHENTICATION EXPERIENCE
Leverages Single Sign On to retrieve secure messages

E. SUPPORTS LARGE FILES
Sends encrypted large files – like financial e-statements or patient records
METHODOLGY

For this study, two surveys were conducted:

I. Enterprise Encryption and Authentication Survey

Primary market research for this survey, on behalf of Echoworx, was conducted by Osterman Research. The survey posed questions to encryption-focused decision-makers and influencers at organizations of various sizes. Questions centred on their organization’s plans for encryption adoption, two-factor authentication and other related issues. The Osterman Research survey panel provided results from a total of 165 surveys taken during September 2016.

ii. Getting Personal Dating Survey

The study, commissioned by Echoworx was conducted by market research company OnePoll in August 2017. This random double-opt-in survey polled 2,000 adults from across the United States. The research asked people to rate their level of comfort in giving out certain sensitive details in different contexts.
As a pure-play encryption solutions provider, Echoworx works with banking, financial service, government, healthcare, legal, and compliance professionals to tailor secure communication solutions that don't impede on customer experience. Our encryption experts take pride in transforming chaos into order for leading multi-national enterprises through our data centers in the U.S., Canada, Ireland, Mexico, and the U.K.