There is an oft-quoted phrase, “better safe than sorry”, that originated from Irish novelist Samuel Lover’s *Rory O’ More* (1837). As with most cliché adages, I have always found it more useful to heed them than otherwise; and, in our brave new world, this phrase rings especially true. Against the backdrop of modern information security, cost of software is usually determined by three tenets: convenience or ease of use, functionality, and security. In a world now seduced, and rightfully so, by the convenience, ease of use, functionality and low cost of mobile storage, the more informed amongst us have grown increasingly concerned with the tradeoff to make such a technological wonder possible: Security.

In contemporary businesses, especially small and medium sized businesses, it is extremely costly and taxing on both financial and manpower resources to enforce and implement a dedicated security infrastructure to safeguard and segment corporate data. With the proliferation of mobile devices such as smartphones, tablets, cloud storage and thumb drives, it becomes not only costly to police data security, but also it may actually be counter-productive; limiting the flexibility and productivity that such devices and software can provide. Implementing a blanket ban on such devices and software is both futile and unnecessary. However, there are still various security risks attached to these devices and software that need to be addressed.

My own experience validates these security concerns. Several years ago, I worked as a freelance web designer. Currently, I am working on various Kickstarter projects with several colleagues. In both cases, there was a similar, pressing need for us to exchange files with one another. However, we faced several problems when doing so. First, one pressing problem with most cloud storage service providers is that they tend to run out of space quickly before the user has to start paying a premium charge. As such, most of us tend to subscribe to multiple providers. This led to various issues, such as one of my team members forgetting the passwords that she used for her different service providers. Our design project was delayed until the provider issued an alternate password for her to use. Although she could have used a single password for all the providers, doing so would have presented its own set of problems. For example, one teammate had his Google password compromised due to a network breach. Since he used the same password for every single provider, he had to change the password of every single service provider to prevent compromise of those other accounts.
Second, for most of the files that we shared, or that we stored in cloud services, we tended not to use encryption. This was primarily a convenience as it is troublesome to run separate third party encryption software, encrypting the files before uploading them to the cloud. When my teammate’s password was compromised, our greatest fear was that the files that we were sharing would be compromised by malicious users. The Kickstarter project that we were working on was projected to be worth around a hundred thousand dollars and we could have lost our prototype designs. Cloud providers do not ameliorate the problem, storage is usually unencrypted, and sharing controlled only by URL access.

Finally, access control rights are not particularly the focus of most cloud service providers. This results in an inefficient and rather brittle trust system, where you trust that the receiving party has a good enough security system, and will not share your file with anyone else. In an early stage team based project, small cells of two to three people share most of the work. Information flow between cells is limited, and designers are rather touchy about intellectual property rights. As the project moves along, people must collaborate across cells, often resulting in a stampeded of copying and deleting files to manually control information propagation and availability.

These problems particularly affect the world of design. In mathematics and science, compared to design, it is easier to see when someone has plagiarize your work. The inner workings are required, by a very rigorous system, to be exposed to the world. Multiple third parties and neutrals are obligated to police such works, and plagiarism can be spotted far more easily. In the murky world of creative works, including web design and prototyping, it is far harder to pinpoint plagiarism. A design that requires months of work and moments of divine inspiration can be easily stolen and edited. No one can detect this plagiarism without exposing the raw, underlying files, and this requires the cooperation of the plagiarizer as well as the original author. The only protection is to prevent the original theft.

However, strict, rigid and heavy-weight security measures bog down work and significantly impede working processes. In this lighting-fast Information Age, such impediment is paramount to a deathblow. On one hand, we are unable to trust anyone; on the other hand, we require fast and efficient flow of information. These two aspects are highly important and paramount, yet most service providers are unable to resolve this issue.
This is where Ohanae can assist, especially for small to medium businesses like the ones I am involved in. My first problem of utilization of different cloud service storage providers can be solved by Ohanae’s patent-pending technology. The Ohanae technology allows encryption keys to be regenerated on demand, based on a user chosen passphrase and a device. This ensures that files may not be accessed and login passwords may not be regenerated without the user passphrase. Conversely, even if the user’s passphrase is compromised, an attacker cannot access files or passwords, even if he or she has access to another system with Ohanae installed on it. This requires the attacker to possess two crucial assets: the user passphrase, and the specific device (e.g. my laptop), before he or she is able to compromise the system. Using such multi-factor authentication, the options of an attacker will be severely limited.

Ohanae 10-Tap Login secure credential management also addresses my first problem. Passwords are generated using the Ohanae patent pending technology, device specific information, user specific information, site or application specific information and history specific counters. These are combined to create a data pool from which Ohanae will select password. Once generated and set on the target site, Ohanae software allows automatic login to the site via 1-Tap functionality where the password and user fields are auto-filled. 1-Tap ensures that I can have arbitrarily complex and individual passwords on each side (preventing any form of dictionary or brute force attacks) based off a single passphrase. Although the core functionality is similar to password managers, these managers do not take into account data access and data protection. They assume that data access is controlled via user credentials, and these credentials will be kept safe. This is, however, insufficient for security. There could be unauthorized credential compromise by network breaches, which is very prevalent (it happened to a teammate of mine as mentioned above), which alone will grant access to user data. However, Ohanae requires both the passphrase and the actual physical device in order to be compromised, thus adding an extra layer of durability to the security.

Ohanae is also able to address the problem of encryption of files. Ohanae secure file sharing augments the simple cloud service provider mechanisms for sharing files. Ohanae provides PKI-based encryption capabilities for transmission of shared data between my teammates and I. The files can be modified and seamlessly re-encrypted for re-transmission. Designing projects require intense and frequent collaborations and modifications. Ohanae’s low-impact encryption, requiring only a simple click to encrypt or decrypt, extends easy, secure sharing to a wide range of cloud service providers that we use, such as Dropbox, Google Drive, OneDrive, and Box. Other file encryption solutions allow encrypting file before sharing, but ignore login authentication. Ohanae’s one stop approach that addresses password logins as well as encryption provides a comprehensive and elegantly simple solution to my requirements around cloud privacy protection.
Finally, Ohanae supports segmentation of user access to files. The file sharing system allows a list of allowed users to be integrated into the file content, and this list can be modified anytime to add or delete users as required. The originator can control these modifications to prevent unauthorized forwarding without notification. As compared to the trust and pact system that my team has used in the past, this leaves far less in the dicey hands of man, and gives the originator a greater degree of control as to the access to his or her files.

In the case of my team, Ohanae is able to provide a device-centric combined solution for both login and data protection. Furthermore it has a wide range of support, extending to third party software that my team and I frequently use, allowing us to protect our data and logins through industry standard, high strength encryption yet allowing us the flexibility to use our own software and devices. With Ohanae, there is no need for data migration, no need for multiple installations of third party software. It is a one stop solution that seamlessly integrates our applications and devices together, for us to securely do our business.

Perhaps the greatest danger and slight in my industry, is having a very personal work plagiarized. It has led to various misunderstandings and fallouts between team mates as each of them accused one another of leaking information. In small and medium businesses, these relationships are the core of the businesses, having sour relationships is one of main reasons why collaborations fail. In this world, trust no one, encrypt everything. By being safe rather than sorry, by encrypting our data using Ohanae, we are perhaps able to set aside any potential for misunderstandings, any suspected violations of our rights. By not trusting anyone, by encrypting everything, we are paradoxically taking a step towards a better world where people can actually trust each other. And when that day comes, my team and I will thank Ohanae.