QATAR CENTRAL BANK

Using Encryptics to Secure Financial Data Nationally

CASE STUDY

Qatar Central Bank and 5 affiliated banking institutions in Qatar are using Encryptics to proactively secure their digital information and prevent data loss.

Goals

- To secure all digital banking and financial information sent via email and stored on external devices.
- To ensure that only authorized personnel have access to the organization's devices.
- To proactively raise the level of security while minimizing the impact to the employees' normal workflow.

Requirements

- Scalable, cost-effective solution that can be used to communicate internally and externally in any email environment
- Email support on various operating systems (Windows, Mac, iOS, and Android)

Solution

- Encryptics for Email
- Policy Based Protection (PBP)
- File Integrity Protection (FIP)
- Multi-factor Authentication (MFA)

Benefits

- **Data Rights Mangement (DRM):** prevent recipients from forwarding, copying, printing, and saving emails
- **Access Controls:** restrict access, set expirations, or recall emails in real time
- **Cross-Platform Support:** use on a range of mobile and desktop devices with any existing email address
- **PBP Rules:** ensure that sensitive data is properly secured
- **FIP:** ensure that attachments conform to document specifications
- **MFA:** ensure that only authorized users have access to corporate devices

Situation

A country's central banking institution is responsible for maintaining the stability of its currency, commodities, and services across their banking and financial institutions. In addition, they are responsible for a variety of macroeconomic and development objectives that are consistent with their government's policies. Internally, access to all devices must be managed and monitored at the highest security level possible to ensure that only authorized personnel have access to critical data and networks. It is also crucially important that they maintain control of their data when it must be shared with external partners and clients around the world.

In an effort to ensure the protection of our financial information, all banking institutions must encrypt their email by the end of 2015.

- His Excellency Sheikh Abdulla Bin Saoud Al-Thani, Governor of Qatar Central Bank

Security Problem

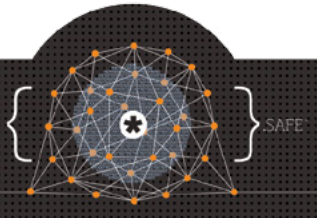
Collaboration between financial agencies can be a challenge and most organizations rely heavily on email as an efficient way to facilitate communication. However, email is highly vulnerable to cyber attacks, and any data sent via email is at risk of being leaked or stolen. If critical financial data falls into the wrong hands, a country's economic security could be in jeopardy.

Once sent, copies of an email proliferate across cyberspace and eventually reside on private servers and user devices all over the world. Worse yet, there is no way to reclaim this data, making these prime targets for cyber criminals and hacktivist groups. Equally troubling, recipients of critical data are free to forward, copy, print, or save these emails without the sender's knowledge or permission. Traditional email encryption products solve these issues by requiring expensive hardware, forcing complex key management solutions, and/or leaving the encrypted data on the same server that holds the keys. Organizations need a more economical, easier, and secure way to protect their data.

Email also remains the primary channel through which Advanced Persistent Threats (APTs) are initiated, with most of these attacks using file attachments to breach an organization's security perimeter. Traditional virus and malware solutions provide reactive protection, meaning they only stop the issues that were in the latest virus definition list. With the frequency of attacks increasing and the cost of incident response rising, institutions need a new, proactive approach to protection that focuses on ensuring the integrity of a file without slowing down the business through excessive use of file quarantining.

Passwords are the most common form of authentication used in the world today. Unfortunately, passwords are also the weakest form of authentication and the most cumbersome to maintain. If an individual can easily gain access to a device carrying critical data, the entire machine and all of its contents can be compromised.

ENCRYPTICS®



Encryptics Solution

Aware of the potential cyber attacks, the QCB sought a security solution that would proactively protect critical data from unauthorized access and inadvertent sharing. After adopting Encryptics defense-in-depth approach to security, the QCB and its affiliated organizations were able to secure the content of more than 700 devices, encrypt email, proactively prevent data loss, and reduce exposure to malware.

By implementing Encryptics multi-factor authentication solution, administrators can require multiple forms of identification to ensure that only authorized personnel can access corporate applications, devices, and networks.

With Encryptics for Email, employees can now easily secure email messages and attachments before sending. The convenient Encryptics' Add-In for Outlook makes securing email a simple, one-click process. Data authors can prevent Forward, Copy, Print, and Save functions on recipient devices and recall sent messages anytime.

For added protection, IT administrators are using Encryptics' Policy Based Protection feature to ensure that data that matches their pre-defined policies is encrypted before it leaves their employees' devices and corporate network. In addition, Encryptics' File Integrity Protection is being used to proactively scan incoming and outgoing email file attachments and cleanse them of malicious code before the intended recipients can open them and become compromised.

Central Bank
Central Securities Depository
Credit Bureau
Financial Centre Regulatory Authority
Financial Information Unit
Financial Markets Authority

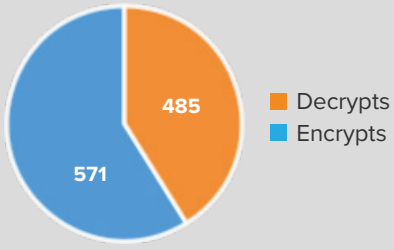
Result

Utilizing advanced data encryption, powerful DRM, customized policies, file integrity protection, and multi-factor authentication provided by Encryptics, the QCB was able to proactively secure corporate assets and financial data.

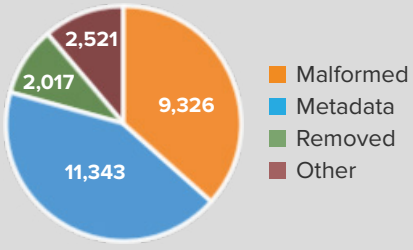
Implementing a protect the data first approach to security and Encryptics defense-in-depth solution, has enabled the QCB to set a new standard for cyber security in Qatar's financial industry.

Proactive Protection Statistics

SAFE File Usage
1,056 Authentications



FIP Usage
25,207 Risks Detected



* Statistics gathered from 01/01/2015 - 04/30/2015

- **True end-to-end data protection**
- **Real-time, agency-controlled DRM**
- **Cross-platform and mobile support**
- **Easy to use**
- **Multi-factor authentication**
- **Policy Based Protection**
- **File Integrity Protection**

About Encryptics

Encryptics empowers data owners—be that an individual or an agency—by delivering true end-to-end privacy and security solutions. Utilizing a proven, multi-layered encryption and data management platform, these solutions eliminate security risks associated with e-communication, cloud sharing, mobility, and more.

Public and private sector entities across industries rely on Encryptics "protect the data first" approach to secure their critical data from leaks and cyber attacks.

visit us on the web
ENCRYPTICS.COM
talk with us
512.649.8185

ENCRYPTICS

QATAR CENTRAL BANK