CASE STUDY

Using Encryptics to Secure Critical Intel during Detroit Gang Threat Investigation

detroitcrime COMMISSION

Goals

- Utilize email to safely share critical intel related to the investigation
- Prevent dissemination of critical intel outside the investigative group

Challenges

- Secure communication between local, state, federal and private-sector agencies
- Risk of cyber-attacks and leaks; exposure of critical intel

Requirements

- Scalable, cost-effective solution that can be used to communicate with any agency in any email environment
- Support for various network devices (smart phones, tablets, message boards, etc.)

Solution

- Encryptics for Email™

Benefits

- **Usage controls:** 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

More than 80 confidential emails secured by Encryptics® to protect details of a highly-publicized case involving the Detroit Police Chief.

Situation

When a death threat was made against Detroit Police Chief James Craig in February of 2014, the Detroit Police Department (PD) rallied troops of investigators to identify those involved and uncover the criminal network behind the threat.

The investigative group included the Detroit Crime Commission (DCC), a nonprofit law enforcement agency serving southeast Michigan. Working with the Federal Bureau of Investigation, the Michigan State Police, the Drug Enforcement Administration, and the U.S. Attorney's Office, the DCC supported the investigation by providing suspect analysis and other critical intel.

Much of the communication among investigators was handled via email. In particular, DCC sent intel reports and other confidential data via email to select members of the investigative group.

Detroit Crime Commission
Michigan State Police
U.S. Attorney's Office
Federal Bureau of Investigation
Drug Enforcement Administration

Security Problem

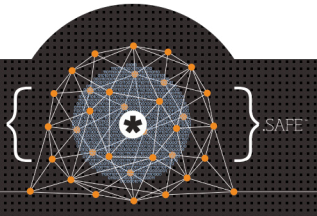
Collaboration between local, state, federal and private-sector agencies can be a challenge, and many investigations rely heavily on email as a quick and efficient way to facilitate communication, especially among bureaucratically diverse entities.

However, email is highly vulnerable to cyber-attacks, and any data sent via email is at risk of being leaked or stolen. If details of an investigation are compromised, critical intel could fall into the wrong hands, putting public safety 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 intel are free to forward, copy, print, or save these emails without the sender's knowledge or permission. And if a laptop, tablet, or smart phone carrying critical intel goes missing, the entire investigation can be compromised.

ENCRYPTICS



More than 80 confidential emails secured by Encryptics® to protect details of a highly-publicized case involving the Detroit Police Chief.

Encryptics for Email Solution

Aware of the risks associated with email, the DCC sought an email security solution that would protect critical intel from unauthorized viewing or inadvertent sharing outside the investigative group. After adopting Encryptics for Email, the DCC was able to secure the content of more than 80 confidential emails, as well as attachments, related to the Detroit gang threat investigation.

Especially useful was Encryptics for Email's Data Rights Management (DRM), which enabled DCC to control how recipients could handle emails containing critical intel. With DRM, investigators at DCC could restrict recipient access; prevent forward, copy, print, and save functions; set file expirations; or recall sent emails at any time.

"

Encryptics is ideal because we can control the flow of information. During the Chief of Police threat investigation, we had designated officers and investigators we were communicating with. When sending intel reports and other sensitive information, we needed to be sure that it was never disclosed to unauthorized personnel–which can include anonymous hackers as well as officers outside the investigation and members of the general public.

Cyber-attacks and even accidental disclosures are becoming far too common, and we feel it is our duty to protect all of the sensitive information we send out. We see great value in the Encryptics for Email product, and that's why we're using it at DCC. Not only does this product work to secure sensitive information, but it provides us an additional level of control where recipients cannot access, alter, export, or share any emailed materials unless we allow it. This is the only way to truly keep sensitive information out of the wrong hands.

-Lyle Dungy, Director of Intelligence, Detroit Crime Commission

Result

Utilizing advanced data encryption and powerful DRM provided by Encryptics for Email, the DCC was able to communicate securely with members of the investigative group and avoid unauthorized dissemination of critical intel related to the Detroit gang threat investigation. DCC's use of Encryptics for Email during this investigation sets a new precedent for cybersecurity in public safety.

DCC Mission

The mission of the Detroit Crime Commission is to lessen the burdens of government and the citizens of the southeast Michigan area by facilitating the prevention, investigation, and prosecution of crime. With special emphasis on criminal enterprises in the metropolitan Detroit area, the DCC conducts research, assists in investigations, disseminates information to the public, and helps coordinate crime reduction activities between business, the public, government, and law enforcement. The DCC also assists in law enforcement training and makes grants to governmental entities to fund law enforcement activities.

detroitcrimecommission.org

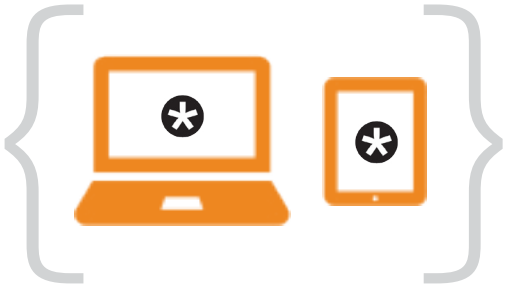
- True end-to-end data protection
- Real-time, agency-controlled DRM
- Cross-platform and mobile support
- Easy to use, software-based solution

About Encryptics Software

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 solutions to protect their critical data from leaks and cyber-attacks.

visit us on the web
ENCRYPTICS.COM
talk with us
877.503.4781



ENCRYPTICS®

detroitcrime COMMISSION