Keeping the Secret Recipe Safe: Why John Podesta's Risotto Matters to Security Professionals Everywhere

The right ingredients for improved email protection are essential, now more than ever

If you add ¼ to ½ cup of liquid at a time—you can get creamy risotto.

How do we know this secret? The same way everyone in the world knows. John Podesta's private email account was victim of a hack and data breach. It started with a spear phishing email sent to the Chairman of the Clinton Campaign's DNC email account on March 19, 2016. It's the risotto recipe heard 'round the world.

The New York Times reported that for nearly seven months before the risotto recipe secret was exposed, the Russians hacked the DNC. A Podesta aide noticed a suspicious email requesting a password change and sent it to a computer tech to validate. And here's where it got worse: The tech said it was legit and the password should be changed immediately. This error opened the door to John Podesta's PII and around 60,000 private emails—that's how we got the tip about creamy risotto. If this could happen to the author of a 2014 report on cybersecurity, it can happen to any public or private organization—unless you're protected.

The hack and breach of a risotto recipe may seem funny, but the protection of intellectual property is no laughing matter. The thousands of DNC confidential emails and attachments published by WikiLeaks changed the world—and as we've seen from the latest WikiLeaks hack, Podesta isn't the only one vulnerable. According to the 2016 Ponemon Institute *Global Encryption Trends Study*, over 50 percent of threats to confidential data come from employee mistakes and nearly 30 percent are from hacks. In the DNC case—it was a double whammy.

We shouldn't be focusing on a risotto recipe. We should be focusing on a SaaS recipe for persistent protection of confidential information at rest, in transit and in use—a solution that delivers encrypted email and document collaboration services anytime, anywhere, on any mobile, laptop or desktop PC device, on any platform.

GigaTrust™ has the secret sauce—the first and only secure email and document protection, consumption, and collaboration service powered by Microsoft – Active Directory Rights Management Services (AD RMS), providing a rights account certificate (RAC) to secure content. GigaCloud™ delivers full control on who can print, forward or edit information with a secure private key. If the DNC had GigaCloud, the risotto recipe would still be Podesta's property with his rights assigned. It's that simple.

GigaCloud Recipe for Success:

1. Two configurations:
    - Hybrid cloud through Microsoft Azure

- On-premise deployments using Azure Stacks or Hyper-V

2. FIPS 140–2 compliant and supports 2 different modes of cryptographic operation:

- Cryptographic Mode 1 by default supports RSA 1024 for signature and encryption, and SHA-1 for signature

- Cryptographic Mode 2, supports RSA 2048 for signature and encryption, and SHA-256 for signature

3. Data OverWatch

- Provides an alert when a breach is attempted

- Captures IP address/time

Don’t let hackers get to your intellectual property. You need to be in control of who has rights to see your confidential emails and documents. The best recipe for content protection is GigaCloud.