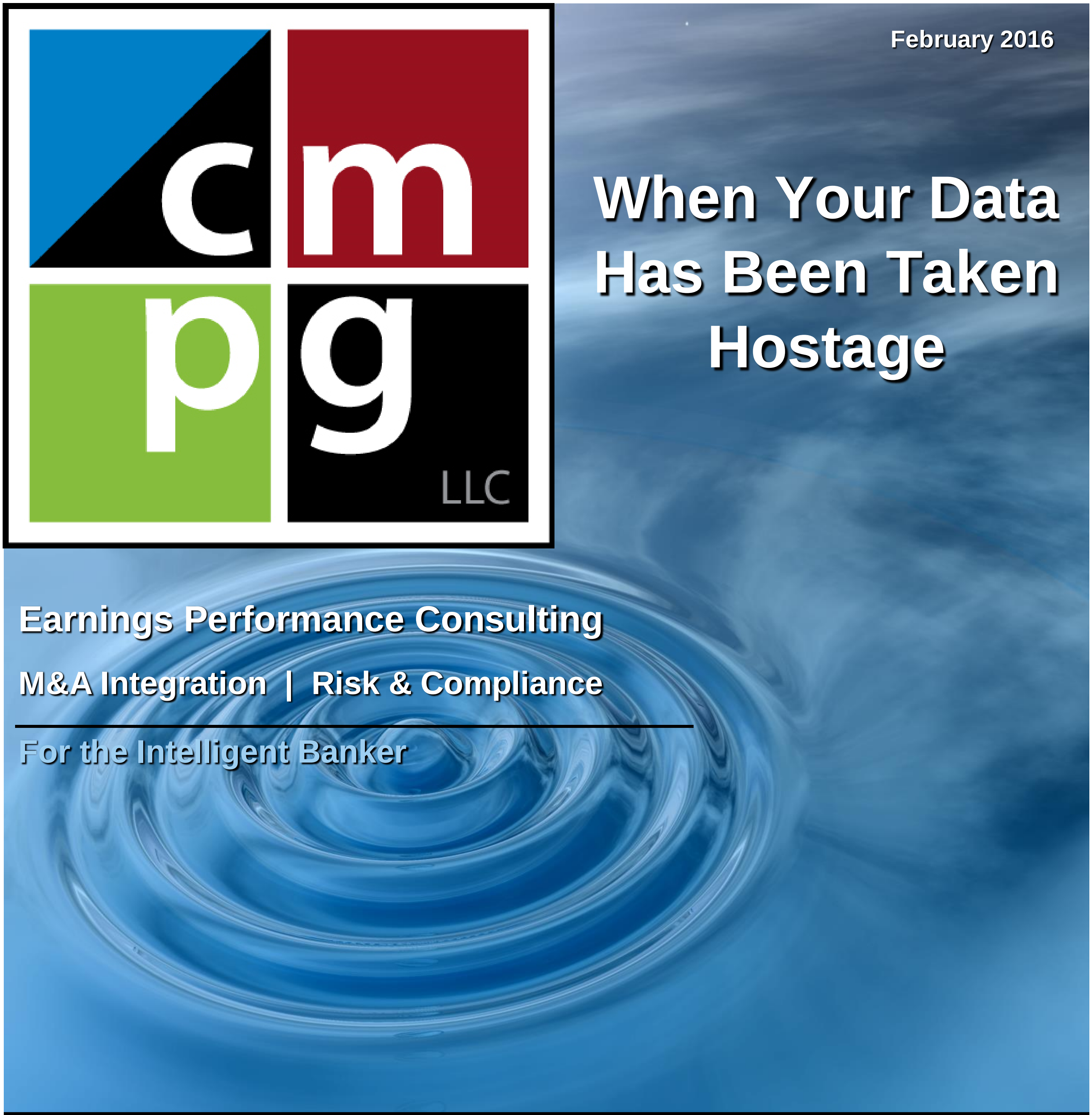
February 2016



When Your Data Has Been Taken Hostage

Earnings Performance Consulting

M&A Integration | Risk & Compliance

For the Intelligent Banker

2016 Intelligent Bank Management Series

The 2016 Intelligent Bank Management Series focuses on insights, strategies and development priorities for improved profitability, operating efficiency, compliance and risk management at U.S. financial institutions.

When Your Data Has Been Taken Hostage.

Learn more about how CMPG can assist you at

www.cmpg.com

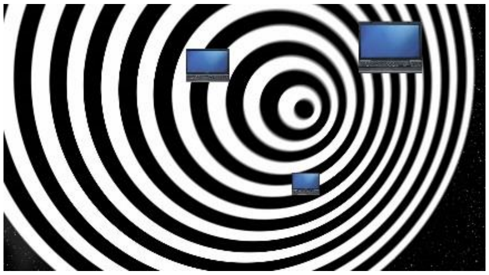
or call us at

1-800-997-2674

to discuss the needs of your financial institution.

Despite all efforts to detect and secure processing environments, businesses continue to experience an increase in malicious software attempts and invasions of their IT systems and networks. We explore the current trends and our recommendations for one of the most potentially damaging breaches; Ransomware.

Imagine yourself in your office at the start of the morning. With your coffee in hand, you awaken your computer to start your day's activities. For some reason, you notice your computer seems slow, or maybe is not reacting to your commands as it has during your entire tenure on the job. Any attempt to open your files is met with an error message from your operating system that the file is not recognized. After a few moments a cryptic screen appears possibly written in a foreign language or alphabet stating your files are locked with unbreakable encryption. It may even present itself as a lockdown of your computer from a spoofed federal law enforcement agency. What is going on, you ask yourself? You are about to enter a new dimension (Rod Serling inflection intended). You have been infected with Ransomware.



What is Ransomware?

Ransomware is a consolidation of the words 'ransom' and soft-'ware', and it is exactly as the two words describe; software designed to infiltrate and hold your computer and files hostage until you pay a ransom. Ransomware does this by encrypting all of the data files on your computer (or network) with strong, virtually unbreakable encryption. It then displays a ransom note informing you where you can make an online payment in untraceable digital currency (typically in

Bitcoins) to receive a decryption key and instructions to decrypt and restore your files. You are often under the pressure of time before the encryption key is erased and any hope of recovering your files is forgone. In this modern day and age businesses and individuals worldwide are routinely confronting this genre of digital terrorism and extortion, though many refuse to discuss the topic. The concern and specified actions we attempt to convey in this article are as result of the need to raise awareness and Cyber defenses from the risk of exposure to Ransomware extortion.

Why is this so dangerous?

Cybersecurity is the defense against individual or organized efforts to gain unauthorized access or disrupt business functionality of services connected to the Internet. Sophisticated solutions and technologies are deployed within Financial Institutions and businesses to prevent or detect and mitigate attempts to gain unauthorized access or overload websites with malicious intent. There are even cases where a ransom is extorted to pre-empt an attack upon a business website, but Ransomware addressed in this article is a different type of digital terrorism and extortion. With Ransomware, the infiltration of the malicious software is not designed to steal your files, but to prevent you from accessing your own computer's contents until you tender payment for the decryption key to restore data access. Ransomware infections most often occur innocently in the normal course of business. Your immediate response may be that you already have in place strong anti-virus and anti-malware protections and these solutions are designed to prevent users from visiting or downloading files from unauthorized or even nefarious websites. But what if the infection has occurred at a business with whom you routinely exchange files and e-mails? Their infection can become your infection.

Of concern is the increasing sophistication as to how these intrusions are being perpetrated. Targeted initially at individual users where in isolation this infection can be devastating, now with the interconnectivity of computers, Ransomware can easily be unleashed on business networks and access and encrypt shared data on network drives and backup drives. It can possibly maliciously encrypt any data resources to which the infected user has access.

Introduce an undetectable, self-replicating virus that moves from the "Patient Zero" infected user device to other network devices, and this scenario gets very scary. A network-wide "Write once – infect all" pandemic infection is only theoretically of concern, as we are not yet aware it is known to exist, but there is evidence that it is a likely future event. A recent article defined how JavaScript has been used to create Ransomware, with the potential to operate undetected within web browsers and even across operating platforms (like MAC OS or Linux, in addition to Microsoft). This particularly dangerous JavaScript Ransomware is being sold on the dark web as a service solution offering to Cybercriminals[1]. JavaScript is utilized ubiquitously today across internet web sites.

What should you do?

When you realize that you have a Ransomware infection, the most important first step is to turn off and isolate the individual machine known to be the infection source. Unfortunately, unless your anti-virus catches Ransomware executing (which most don't), you may only become aware of your infection as result of shared network resources becoming encrypted and unavailable. Ransomware is always configured to do its work quietly behind the scenes until it is done, and then it presents the ransom demand. In this way it does the maximum damage leaving you completely unable to access any of your files and more likely to concede to the extortion demand. The typical practice of allowing computers to remain up and connected overnight can provide Ransomware the ability to have free rein of network files and resources for extended periods before detection.

Steps to take:

- Identify the "Patient Zero" user that has become infected by evaluating the files that have been encrypted.
    - This is easily accomplished by checking an encrypted file and determining who last accessed and modified it.
    - Compare multiple encrypted files to determine if commonality exists as to who has access rights.
    - If you are unable to quickly determine "Patient Zero" you may consider shutting down all terminals. Yes, the threat is that bad!
- Validate where the infection initiated and collect any evidence regarding the files that have been altered by encryption and the payment demand.
- Shut down this computer immediately upon identification.
- Physically unplug the computer from the network and any wireless devices.
- Assess your back-up status.
    - How many generations of back-ups do you maintain?
    - Do you keep offline backups (i.e. backup sets not connected to the network with no chance of being Ransomware encrypted)?
    - How can you evaluate your back-up files isolated from your network to assess which files have been encrypted nefariously starting with your oldest files first.
    - For Microsoft networks, this is where Shadow Copy can become your best friend. Because Shadow Copy only runs under

Administrator or System rights and credentials, it remains pure from the invading encryption (unless the “Patient Zero” user has been provided Administrator rights and credentials, and then you have a larger concern).

Can you defend against it?

Just like an infection of your body, the earlier you catch it, the less damage can be done. The answer at the moment to defense is little more than awareness and preparedness. Current anti-virus and anti-malware have been shown to do little to detect or prevent these style perpetrations. Criminal intent and software mutations are stronger and more agile than most existing solutions have an ability to detect and respond. The traditional approach of building a castle wall around your network will not prevent malicious content from crossing the moat through the lowered drawbridge and open gate. The key aspect of Ransomware detection is the monitoring of file renaming and changes. Products do exist that monitor anomalies and deviations from the “Known Good”, but these solutions have not been typically deployed at the individual machine level and are only typically found within more sophisticated network deployments. We assert that Operating System providers need to be building their future desktop solutions towards incorporating sensitivity to even miniscule file changes that would indicate the possibility of such an infection, with an ability to systemically stop and isolate computer operations immediately, disable connections and require administrative efforts to resume normal operations.

As an IT Professional, you have an obligation to ensure that your security and support staff are fully aware of the risk of Ransomware. Help Desk technicians need to be acutely prepared to react to the signs of an infection as they talk and work with the distributed user community. Network administrators need to ensure user access and permissions are tightly assigned; be extremely careful where and to whom you provide read/write permission within your network. Access to files and resources need to be on an “as required” basis, with logical (and physical) barriers placed internally to prevent unauthorized access. Your back-up methodology and discipline needs to be exemplary.

As an Executive manager protecting the assets of the bank, you hold the responsibility to ensure that you have fully funded training and solutions as they become available to keep up with detecting and isolating any Ransomware threat. One avenue worth exploring is whether there is an aspect of insurability under a Cybersecurity policy with regards to reconstruction costs.

While this is digital terrorism and extortion, law enforcement will be of little help. Ransoms can be as small as $300-$500, but can be in the tens of thousands of dollars. Some estimates are that Cryptowall (a popular and prevalent strain of Ransomware) netted hackers over $18 million dollars in a little over one year.[2] The position often being espoused by the FBI’s[3] CYBER and Counterintelligence Program is to pay the ransom in order to regain access to your files. To us, this does not make sense as there is no guarantee that payment will lead to unlocked files, or that the criminals that perpetrated your intrusion will be deterred from future attempts to extort you again. This decision will ultimately fall to the highest levels within any organization.

In the end, no one is coming to your rescue or providing you or your organization restitution. It seems the old adage AMF,YOYO is the order (Adios My Friend, You’re On Your Own). As this method of extortion continues to spawn and evolve, clearly this will remain one of those business IT aspects that keeps a good many people up at night for the immediate future.

1 - Cyberheist News; Volume 6 #1 January 5, 2016 First JavaScript-only Ransomware-as a-Service Detected

2-Buisness Insider – October 26, 2015 The FBI says you may need to pay up if hackers infect your computer with ransomware

3 -The Security Ledger – October 10, 2015 FBI’s Advice on Ransomware? Just Pay The Ransom.

To discuss the needs of your financial institution
or learn more about CMPG services:

www.cmpg.com

1-800-997-2674