DIGITAL MOUNTAIN®

FALL 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we focus on the topic of ransomware and the information security, legal and financial impact it has on organizations.

RANSOMWARE - GRAPPLING WITH GROWING HOSTAGE SITUATIONS

On August 3, 2016, the International Olympic Committee honored eleven victims of the Munich Massacre, a hostage situation during the 1972 Summer Olympics that ended tragically, reminding the world of the high-stake and long-lasting impacts of hostage situations. Ransomware, the malicious software that holds critical data and systems hostage through encryption, has not yet taken human life, but it does evoke similar emotions and endanger human life, especially in the context of critical health data that's encrypted and lost forever.

When a hostage situation strikes, the crisis response is directed and controlled by *people* acting with limited time, so it's imperative for organizations to have established relationships with experts to assist before, during, and after emergencies, increasing the likelihood that organizations avoid the tragedies associated with ransomware.

The Floppy Origins[1] of Ransomware

Since 2005, the proliferation of open-source tools for encryption and anonymization have solidified ransomware as a commodity of cybercrime, but the first ransomware was developed twenty-five years ago. The AIDS Trojan, as it came to be known, was malicious software distributed on floppy disks thought to contain information about the disease – instead, it scrambled data and demanded payment be sent to a PO box. Fortunately, security researchers quickly cracked the cipher used to scramble the data and widely distributed it to victims of the AIDS Trojan, minimizing much of the damage. Today's ransomware is much easier to distribute, more technically sophisticated, and has inflicted greater financial damage to its victims.

The Financial Impact of Today's Ransomware

The frequency of ransomware attacks has increased sharply, thereby driving up victims' costs; notably, ransom payments are *not* the only costs incurred by organizations. By the time an organization recognizes it’s been hit with ransomware, broader questions must be answered, possibly leading to further security, administrative, and legal obligations.

Negotiation is common during ransomware attacks, but don’t trust the attacker. A high-profile ransomware attack on a healthcare institution that initially demanded three million dollars ultimately settled for forty bitcoins (worth $17,000 at the time)[2].

The FBI recently estimated that the infamous CryptoWall, a variant of ransomware that evolved from CryptoLocker (an earlier version that was interrupted by law enforcement), had accrued over eighteen million in illegal profits. The FBI further reported that in the first quarter of 2016, profits from ransomware grew to two hundred and nine million, driving up estimates to one billion in profits by the end of 2016.

The Executive Starting Point – Handling Hostage Crises

Executives at organizations fend off threats of varying degrees on various fronts (including from competitors). Executives rely on experts to guide their decision making process. Dealing with ransomware attacks is not much different; it requires an awareness of the threat and the prescience to establish proactive relationships with experts that can usher your organization to safety during a crisis. Experts can prepare organizations to avoid ransomware attacks, assist during ransomware attacks, mitigate losses and remediate systems following a ransomware attack, and assist in determining further obligation resulting from an attack.

If you have an expert in place, ask the following FBI-recommended questions[3] as a baseline for discussion because the answers will provide insight as to the comprehensive nature of your program:

Backups ▪ Do we backup all critical information? ▪ Are the backups stored offline? ▪ Have we tested our ability to revert to backups during an incident?	**Application Whitelisting** ▪ Do we allow only approved programs to run on our networks?
Risk Analysis ▪ Have we conducted a cybersecurity risk analysis of the organization? ▪ If so, was the scope of the analysis broad enough to include all attack vectors?	**Incident Response** ▪ Do we have an incident response plan that includes ransomware and have we exercised it?
Staff Training ▪ Have we trained staff on cybersecurity best practices?	**Business Continuity** ▪ Are we able to sustain business operations without access to certain systems? ▪ If so, for how long? ▪ Have we tested this?
Vulnerability Patching ▪ Have we implemented appropriate patching of known system vulnerabilities?	**Penetration Testing** ▪ Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

In light of the risks ransomware poses to an organization, early threat assessment, proactive data protection, and comprehensive disaster recovery planning aren't just smart, they're essential: essential to the continuation of business, essential to helping stop the commission of cybercrime, and most importantly, essential to the protection of the *people* the data is meant to serve.

Please direct questions and inquiries about ransomware, cybersecurity, and digital forensics to info@digitalmountain.com.

[1] https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf
[2] http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
[3] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf

UPCOMING INDUSTRY EVENTS

October 2016
Privacy + Security Forum,
Washington, DC: October 24-26

The Sedona Conference Working Group 1 on Electronic Document Retention,
Atlanta: October 27-28

November 2016
Georgetown Law's The Advanced EDiscovery Institute,
Washington, DC: November 10-11

December 2016
Association of Defense Counsel Annual Meeting,
San Francisco: December 8-9

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: