# CYBER INCIDENT RESPONSE

This document has been created to assist you in the event of a cyber related incident. This is not intended to describe, explain or otherwise address any applicable insurance coverage or insurance policy terms. Furthermore, the identification of any provider below is for convenience only and is not an endorsement of a vendor's skill or experience. Use of any listed provider is at your sole discretion and you are responsible for any vetting or incurred fees for their services.

## Ransomware Attack – Cyber Extortion

**Ransomware** is a type of crypto virus that essentially holds data on computers hostage by encrypting the files, and making them unusable. The cybercriminals demand a "ransom" payment before potentially restoring access to your files. If the ransom is paid, the cybercriminal promises they will provide a "key" to decrypt the data. The ransoms are typically demanded to be paid in a cryptocurrency such as "Bitcoin." If you believe your systems have been infected with malware and or a crypto virus such as ransomware, you should turn off all of the systems and network devices to prevent the infection from spreading. You should then contact an IT provider to scan your systems.

If your IT provider is going to restore systems, they should preserve an image of the system in case a Forensic IT review is necessary for determination if a breach of personally identifying information may have occurred. Law Enforcement should be notified of any incident involving a computer attack or cyber extortion event.

***Payment of a ransom is not a guarantee that your data will be recovered.***

### Cyber Extortion Negotiation Providers

The following providers can assist with cyber ransom negotiations and the data restoration process**.**

- **Coveware - www.coveware.com 203-442-4050**
- **Crypsis Group – www.crypsisgroup.com 705-570-4103**
- **Kivu Consulting – www.kivuconsulting.com 415-524-7320**

# CYBER INCIDENT RESPONSE

## Data Compromise - Information Privacy

**"Data compromise" or "Information Privacy Event"** is the unintended breach or loss of personally identifying information, personal health information or personal sensitive information such as Social Security Numbers, health information, etc., of employees or customers that is in your care, custody and control, or to a third party that you have turned over this information to on your behalf.

All 50 States have laws in place requiring action on your part to Notify any Affected Individual and the State Attorney General's, when a reportable breach has occurred. You may be required to provide written notice and possibly credit monitoring services to the Affected Individuals. The Health Information Portability and Accountability Act "HIPAA" may also dictate actions for notification and or breach risk analysis.

To determine if a breach has occurred, it may require a Forensic IT review to determine if any information was taken from a computer network or system. In addition, Legal Review may be necessary to determine and provide you with assistance in determining how best to respond to any State laws or Federal Regulations.

### Forensic IT Providers

- **Crypsis Group – www.crypsisgroup.com 705-570-4103**
- **Envista Forensics – www.envistaforensics.com 888-782-3473**
- **Arete Advisors – www.areteadvisorsinc.com 866-210-0955**

### Legal Firms

- **Lewis Brisbois Bisgaard Smith – www.lewisbrisbois.com - 844-312-3961**
- **Jackson Lewis – www.jacksonlewis.com - 844-544-5296**
- **Marshall Dennehey – www.marshalldennehey.com - 800-220-3308**

### Credit Monitoring / Notification Services

- **ID Experts - www.idexpertscorp.com 800-298-7558**
- **Epiq – www.epiqglobal.com**
- **Experian – www.experian.com 714-830-7000**