CHUBB®

Cyber InFocus

August 2019

Know the Latest Trends in Cyber Risks

A surge in Biometric Information Privacy Act ("BIPA") lawsuits and a defined increase in the use of ransomware further proves the need for special attention to an organization's cyber security program. Certain types of ransomware, like malware and ryuk, are more likely to infect system backups so that when the ransomware hits, insureds are forced to pay the ransom. Consistently testing and re-evaluating an organization's incident response plan can go a long way when an incident like this occurs.

BIPA – Surge of Class Actions alleging violation of the Biometric Information Privacy Act

What it is

In 2008, the State of Illinois enacted the BIPA which regulates the collection, use, storage and destruction of a person's "biometric identifiers." BIPA defines "biometric identifiers" as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."

How it works

BIPA requires notice before biometric information is collected, limits the sale and disclosure of biometric information, requires reasonable care to safeguard biometric information, prohibits the retention of biometric information beyond the purpose for which it was collected, and requires that a private entity establish and maintain a retention policy that provides for the permanent destruction of biometric information when the initial purpose for collecting or obtaining such information has been satisfied. BIPA also has rigorous consent requirements. BIPA is currently the only state biometric law that provides for a private right of action. Alleged victims can bring suit on the basis of a technical violation alone, and without the need to prove that they suffered actual damages. Statutory damages of $1,000 for each negligent violation and $5,000 for each intentional or reckless violation can be recovered, along with reasonable attorneys' fees and costs.

Trend

In January of 2019, the Illinois Supreme Court held in *Rosenbach v. Six Flags Entertainment Corp.*, 2019 IL 123186* (Jan 25, 2019), that a technical violation of BIPA, without any additional actual damages, was sufficient to maintain an action brought under BIPA. The decision held that because BIPA vests in individuals the right to control their own biometric information, a violation of the act erodes that right and creates a "real and significant" injury. *Id.* Illinois courts have now seen an increase of BIPA-related litigation.

Chubb Insight

Companies doing business in that state need to be aware of the law's requirements, especially if the company regularly collects biometric information.

iEncrypt – A New Ransomware Variant

What it is

A seemingly sophisticated type of ransomware that was first identified at the end of 2018 where the bad actors demand mid six to seven figure amounts to decrypt a victim's data.

How it works

The bad actors appear to exploit previously compromised credentials that a bad actor obtained from malware placed on a system. They use this existing malware, such as Dridex or Emotet, to get login credentials to enter the victim's computer system. The Dridex or Emotet is introduced via phishing emails. Generally, the bad actor then explores the victim's computer systems extensively before deploying iEncrypt. Once deployed, iEncrypt then acts to encrypt files individually, while also targeting and encrypting the victim's backups.

Trend

Given the ability to target and encrypt backups, victims of iEncrypt are often put in a position to either completely lose their data or pay the six to seven figure demands

Chubb Insight

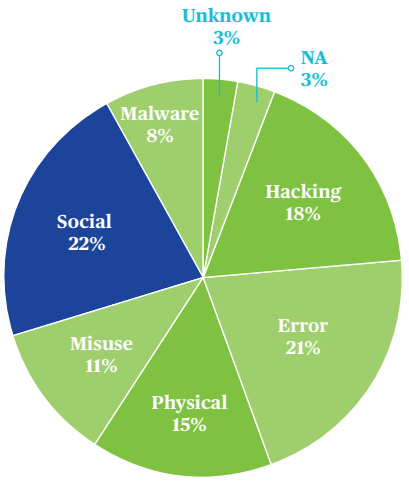
Companies should constantly evaluate and test their security protocols and incident response plan to ensure that they are utilizing the latest malware threat detection systems and can detect Dridex or Emotet, or any other vulnerability to iEncrypt. Additionally, ensuring daily offline backups and testing them regularly, as discussed next, should be a vital part of the Incident Response Plan.

Backups

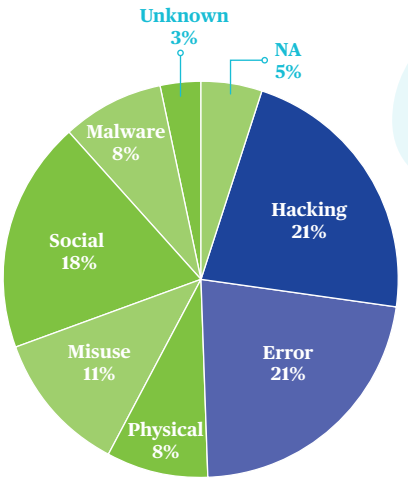
When addressing a ransomware situation, the availability of backups is vital to ensure a proper and effective response. When the victim's main system is encrypted by the malware and unusable, having the ability to access backup information allows the business to resume normal operations as quickly as possible. The time it takes to resume normal operations is vital, as the data has shown that generally the longer it takes a business to get back to work, the higher the remediation expenses and overall losses are. A recently observed and unsettling trend is that certain types of malware are now specifically targeting and scouting for a business' backups, especially when the backups are accessible online. When both the backups and the main system has been held for ransom, a business is left with very few options to confront and resolve the ransomware situation. While there are many different ways to maintain system backups, including keeping them off-line and sometimes even off-site, it is important that businesses structure their systems to enable and protect access to backups, and that they consistently update and maintain current backups (which includes backing up system information on a daily basis).

Spotlight on: Financial Institutions

Human error and often-preventable hacking and phishing attempts continue to top the list of cyber attacks hitting financial institutions. Why are bad actors using these methods to target financial institutions? The robust amount of financial transactions makes these institutions prime targets. By monitoring trends and raising awareness of new threats, we can help our insureds stay informed, so they can reduce their exposure to these types of cyber attacks.



Claim % By Action, 2016-Present



FI Claims by Action in 2019

"The Chubb Cyber Index℠ contains more than two decades of cyber claims data, which enables us to help our clients gain insight into the types of events affecting their industries. This continually updated data showcases the need for financial institutions to take advantage of loss-mitigation services such as employee education and password management software."

Chubb. Insured.℠

[1] SOURCE: Alton, Larry. "How to Protect Your Small Business as Cybersecurity Threats Rise." Small Business Trends: https://smallbiztrends.com/2016/06/cyber-security-strategies.html (June 3, 2016).