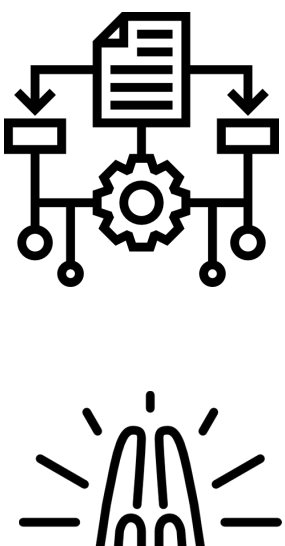
CRYPTO CRIME

Executive Briefing

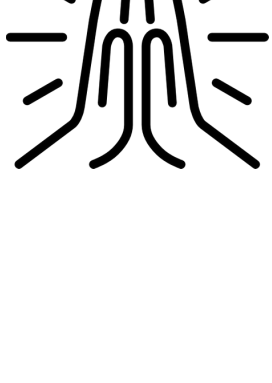
Crypto crime was born in 1989, but it wasn't until Bitcoin and related technologies were released in 2009 that crypto crime began to grow. Here is what you need to do in order to keep your orgaization secure as it faces future crypto crime attacks.

CRYPTO JACKING | RANSOMWARE | CRYPTO PHISHING | ICO SCAMS | CRYPTO THEFT | MONEY LAUNDERING



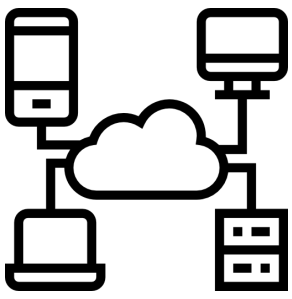
1 BUILT-IN SECURITY

Security must be built into your organization. A risk-based security approach, when properly governed, is essential to laying the ground work for future crypto crime prevention.



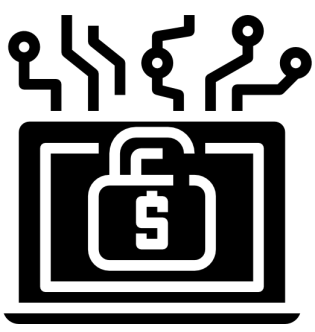
2 A CULTURE OF SECURITY

The human element is typically viewed as the weakest link, but your organization's people can be your best defense. A culture of security is essential to protect your organization from threats such as crypto crimes because sometimes only humans can pick up on the giveaways to these attacks.



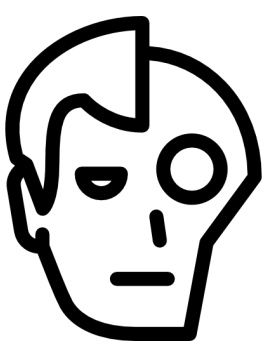
3 DATA MANAGEMNT

Data management is essential. You should have protections for data in use, in transit, and at rest. Backups are essential to protecting against crypto crimes such as ransomware. Backup data consistently, making redundant, air-gapped copies.



4 BUSINESS CONTINUITY PLANNING

Once an attack happens it is imperative that you can recover. You should have an incident response plan and specific "playbooks" for recovering from various attacks. Finally, you should know how much data you could lose and how much downtime you face in the event of an attack. Practice disaster recovery.



5 INSIDER THREATS

Insiders have the potential to cause devastation. There are various reasons why an insider may launch an attack, but the result is always the same, disaster. It is paramount that you operate and maintain an anti-insider threat program at your organization.