# Data Privacy Detective Podcast – Episode 65: Ransomware Basics

May 03, 2021

**Categories:**

Blogs
Podcast
Technology Blog

**Authors:**

Joseph J. Dehner

This podcast episode explores ransomware from preventive, legal, and communications angles. While there's no 100% effective vaccination against a ransomware attack, there are steps enterprises and each of us can take to beware, prepare, and take care.

Ransomware. It's the modern equivalent of kidnapping – except people aren't grabbed and held hostage. Instead, an enterprise has its computer and information system locked by a criminal. Data gets encrypted and unusable until and unless the organization pays a ransom to the thief, who is known only by a digital address and often demands untraceable payment in cryptocurrency.

Ransomware is a type of malware – software installed in a system by an outside party for bad purposes. Unlike malware focused on stealing data, ransomware aims to extract a ransom payment in exchange for decrypting and restoring the victim's data.

From a criminal's perspective, ransomware is a simpler, less expensive way to get money than malware that aims to export (or exfiltrate) and resell data. It can be an "in and out" operation, not requiring search, download, categorization, and reselling of purloined data. Despite this, because data has great value, Blackfog estimates that 70% of ransomware attacks include data exfiltration, so that the attacks not only temporarily freeze data usage but result in a release of personal and business data to third parties as secondary damage. Ransomware Breaches and Class Action Lawsuits (blackfog.com).

Ransomware theft is rising. Security sector experts report a 7-times increase in ransomware attacks between 2019 and 2020, with the average ransom demand increasing more than 3 times the prior year's figure. Blackfog predicts cybersecurity theft will approach $6 trillion for 2021. CrowdStrike's comprehensive summary of 2020 and early 2021 reports a four-fold increase in interactive intrusions in the past two years, with 149 criminal syndicates followed as tracked actors on its list of named adversaries. Ransomware is

organized crime on a massive and global scale. 2021 CrowdStrike Global Threat Report.

For units of government, businesses, and non-profits (like universities and hospitals), ransomware can strike like a rogue wave at sea. But it's often an attack more like a time bomb, lying in wait until the criminal gang is ready to demand its ransom at a time of its choosing. And when this happens, it can immobilize the organization's ability to operate. Immediate action is required. How do we get our data back? Do we pay the ransom? If we do, will we get the data back? Even then, how do we know it's safe? How can we prevent this from happening again? If it does, how do we deal with the immediate issues, recoup the data, and ensure it's clean and usable?

## First – Beware! Prevention tips:

- Personnel training- Limit the risk of a ransomware attack by training anyone who has access to a system about how not to let outsiders in. Create a culture of cybersecurity.
- Partner with peer groups fighting the scourge. Team with law enforcement to learn of emerging threats and attack vectors (e.g., InfraGard — FBI).
- Use multifactor authentication for access to an IT system.
- Appy safety standards to remote work.
- Engage a service providing real-time review of data streams to detect and delete known and emerging malware (e.g., vigilantnow.com)
- Engage in threat hunting through reliable service providers (e.g., crowdstrike.com).
- Consider a threat removal service. Deep Secure, a UK firm, offers what it describes as a "zero-trust approach to real-time, malware-free data exchange." deep-secure.com.
- Continually upgrade to best practices. See, e.g., Ransomware Prevention and Response for CISOs — FBI

## Second – Prepare! Preparation tips:

- Consider cyber insurance, understanding what it does and doesn't cover and how it can provide a systemic plan to address and cover costs of an attack.
- Have a plan and team ready before a crisis hits – including cyber, legal, and communications expertise.
- Practice breathing rather than emoting, so that when a crisis arises, it will be handled intelligently. Be ready with good messaging internally and externally.
- Install a back-up repository of critical data not connected to an organization's IT system (cloud back-up alone may not be disconnected – sophisticated attackers ensure ransomware locks both on-site and cloud-kept data).
- Be ready to meet data breach notification deadlines under national, federal, state, provincial, and local laws (a ransomware attack will almost certainly be deemed a form of data breach).

## Third – Take care! Avoid mistakes in responding to a ransomware attack.

- Paying ransom does not guarantee you will get your data back. The FBI opposes payment of ransom. Ransomware — FBI .
- Don't violate the law in defending against an attack. Paying a sanctioned person or organization anything of value (e.g., cryptocurrency) is illegal and subject to civil and criminal penalties.
- Reputational loss is often greater than the immediate cost of dealing with a ransomware attack.
- Recouping data does not complete a response. Recovered data may bring with it malware or corrupted data.

Personal devices and systems are subject to ransomware attacks, though the ransom demands are much lower than those for enterprises. The same training organizations use for their personnel will educate individuals to protect their home and personal devices and information.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.







FBT Gibbons