

2021

THE ULTIMATE GUIDE TO

Managing Ransomware Risk

bugcrowd






CONTENTS

- 1** Introduction
- 2** Understanding Ransomware
- 3** How Big is the Ransomware Threat to You?
- 4** Five Best Practices for Safeguarding Against Ransomware Attack
- 6** Crowdsourced Security Can Help
- 6** Recommendations

INTRODUCTION

A woman with blonde hair is looking at a laptop screen. The laptop screen shows the Apple logo. The background is dark with some light streaks.

Ransomware is a form of malware engineered to encrypt files so they are inaccessible. This encryption renders all of the systems that rely on them totally unusable. In fact, your data is likely exfiltrated and stolen before it is encrypted. In 2020, **half of the ransomware attacks were preceded by theft of the data**¹. This gives threat actors **twice the leverage** so they can deliver a solid one-two punch. First, you need to pay them to get the encryption key to unlock your files. Second, if you don't pay, they will publish all of your confidential and internal data on the public facing internet.

Ransomware is not hard to find. It can be as simple as a business partner or employee just clicking on an email attachment. At that moment, the malware can infect their computer and then start moving across the local network encrypting and locking all of the files as it goes. The **ominous grand finale** is that the ransomware covers your monitor with a splash screen declaring that a ransom must be paid by you to regain access to your files.

This guide takes a closer look at **ransomware threats**. Unfortunately, there is nothing an organization can do to fully guarantee avoiding ransomware, but there are steps you can take to better protect yourself.

¹ <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

UNDERSTANDING RANSOMWARE

If successful, ransomware attacks can extort your funds, damage your reputation and brand, and shut down or severely degrade your operations for a sustained period of time resulting in additional loss of revenue, customers, or much worse.

The numbers on ransomware attacks are grim. It all starts with the vulnerabilities in your infrastructure. From 2019 to 2020, we've seen a **4x increase in the vulnerabilities tied to ransomware**. This gives threat actors 4x the attack plane to target. There are over **15 ransomware families** alone identified on ransomware-as-a-service websites and over **124 current trending ransomware attackers**².

Worse yet, at the end of 2020, the average ransom payment reached an average of \$233,817 which reflected significant growth over 2019.

This was accompanied by an **average of 19 days of downtime due to the ransomware attack**. As an example of the potential damage, it is estimated that WannaCry ransomware caused over **\$4 billion in damage** to organizations in just a few short years.

The leading ransomware attack vectors have targeted exploiting the **remote desktop protocol** (RDP) of medium to small-sized businesses. In particular, these organizations often don't seem to have any protection in place. In some cases, the exploited organization did not even know that they had an RDP server exposed in the public domain. **Email phishing** is very successful in targeting large to enterprise class government agencies and businesses.

It is important to realize that if you pay the ransom, it is far from guaranteed that the threat actors will provide you with the encryption key. Threat actors may instead demand additional funds from organizations that have already paid the original ransom. The FBI has noted that this **"Pay Me Now - Pay Me Later"** scenario happens frequently to many organizations that paid the ransom.

² <https://www.prnewswire.com/news-releases/as-the-cost-of-ransomware-attacks-nearly-double-lumen-deploys-program-that-helps-businesses-fight-ransomware-before-it-strikes-301264666.html>



HOW BIG IS THE RANSOMWARE THREAT TO YOU?

The U.S. deputy attorney general, Lisa Monaco, warned that U.S. businesses need to **prepare for a very large increase in the number of ransomware attacks** being made by criminal threat actors and hostile nation states, or in some cases a blended collaborative threat of both. “The message... to the CEO’s around the country, is that you’ve got to be on notice of the exponential increase of these attacks,” Lisa Monaco said.

For every attack that is visible in the public domain, there may be 30 other attacks which are not publicized.

The recent cyberattacks on Colonial Pipeline and the meat processing company JBS were reflective of the sorts of intrusions taking place every day.

FBI Director, Christopher Wray, says the FBI is investigating roughly **100 types of ransomware**³. Director Wray noted that the attacks on Colonial Pipeline and JBS have parallels to the scale of challenges surrounding the terrorist attacks on 9/11.

According to a recent **White House memo** published in early June, **“The threats are serious and they are increasing,”** Ann Neuberger said, President Joe Biden’s deputy national security advisor for cyber and emerging technology. Neuberger further noted that, “All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location.”

“ All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. ”

³ <https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003>



THE FIVE BEST PRACTICES FOR SAFEGUARDING AGAINST RANSOMWARE ATTACK

The White House stepped up and listed the five best practices for safeguarding against a successful ransomware attack. They include:



1. CHECK YOUR SECURITY TEAM'S WORK

Use a third party **pen tester** to test the security of your systems and your ability to **defend against asophisticated attack**. Many ransomware criminals are aggressive and sophisticated and will find the equivalent of unlocked doors. Learn more about pen testing in [The Ultimate Guide to Penetration Testing](#).



2. SEGMENT YOUR NETWORKS

There's been a recent shift in ransomware attacks – from **stealing data to disrupting operations**. It's critically important that your corporate business functions and manufacturing/production operations are separated and that you carefully filter and limit internet access to operational networks, identify links between these networks, and develop workarounds or manual controls to ensure ICS networks can be isolated and continue operating if your corporate network is compromised. **Regularly test contingency plans** such as manual controls so that safety-critical functions can be maintained during a cyber incident.

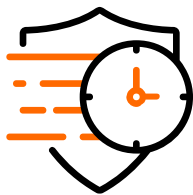


THE FIVE BEST PRACTICES FOR SAFEGUARDING AGAINST RANSOMWARE ATTACK



3. BACKUP YOUR DATA, SYSTEM IMAGES, AND CONFIGURATIONS, REGULARLY TEST THEM, AND KEEP THE BACKUPS OFFLINE

Ensure that backups are regularly tested and that they are not connected to the business network, as many ransomware variants try to find and encrypt or delete accessible backups. **Maintaining current backups offline** is critical because if your network data is encrypted with ransomware, your organization can restore systems.



4. UPDATE AND PATCH SYSTEMS PROMPTLY

This includes maintaining the security of operating systems, applications, and firmware in a timely manner. Consider using a **centralized patch management system**; use a **risk-based assessment strategy** to drive your patch management program.



5. TEST YOUR INCIDENT RESPONSE PLAN

There's nothing that shows the gaps in plans more than testing them. Run through some **core questions** and use those to **build an incident response plan**: Are you able to sustain business operations without access to certain systems? For how long? Would you turn off your manufacturing operations if business systems such as billing were offline?



CROWDSOURCED SECURITY CAN HELP

Your organization can move faster to decisively leverage the **benefits of penetration testing** per the White House recommendations. Any sized business can do this by using Bugcrowd's network of on-demand ethical hackers (**The Crowd**). Bugcrowd's ethical hackers are distributed across the world and connected via the Bugcrowd platform.

The Crowd powering this new type of security testing includes security researchers, from academics with advanced degrees, professionals who hack as a hobby, to self-taught hackers virtually anywhere in the world. They are all united by their ability to

demonstrate **tangible results in security testing**.

Crowdsourced security allows organizations to tap into expert testing at any level of scale. Crowdsourced security allows organizations to deploy a suite of advanced security testing methods while defining the scope, compensation model, and timeline that is tailored entirely to their independent way of working. Crowdsourced security moves faster, enables more **highly skilled resources**, and produces perhaps the most **accurate and comprehensive results**. Crowdsourced security also **reduces risk** - it is used by firms such as Google, Facebook, and Apple.

RECOMMENDATION

Ransomware risk management needs to become a central part of every organization's operations. Threat actors are sophisticated, highly capable, and able to cause harm to any organization that has the open and exposed vulnerabilities.

If you would like to know more about accelerating ransomware risk management using crowdsourced security, Bugcrowd can help.

Learn why companies turn to Bugcrowd for crowdsourced security www.bugcrowd.com/get-started

