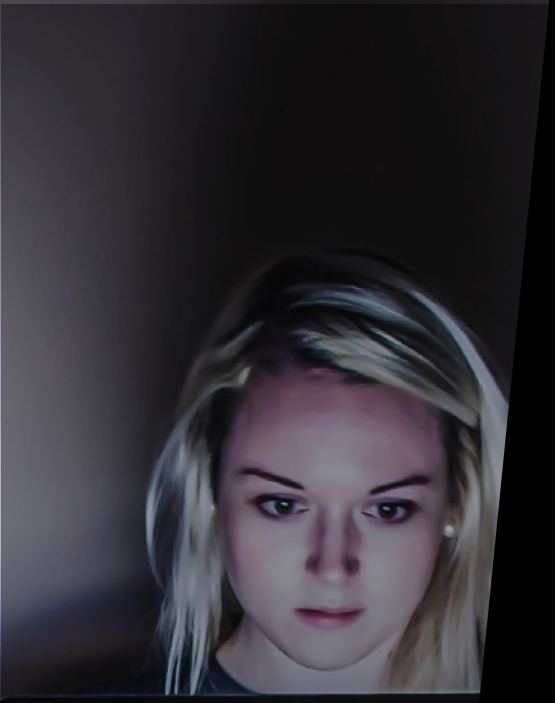
ULTIMATE GUIDE TO

Managing Ransomware Risk

bugcrowd SOFTPROM

CONTENTS



INTRODUCTION

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.** Whereas in the past, ransomware threats were most common for smaller companies, in 2021, the "ransomware as a service" industry discovered that the same tactics, techniques, and procedures (TTPs) that work on small targets are just as effective on larger, more well-financed ones. As a result, in 2022, 37% of all businesses and organizations were affected by ransomware in some way (reported cases only).

Ransomware is not hard to find. An attack 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 you must pay a ransom to regain access to your files. Although 77% of attacks involve the threat to leak stolen data, even if you pay the ransom, your data is likely to end up in the wrong hands anyway or even held for future extortion.

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

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 or customers or much worse.

The numbers on ransomware attacks are grim. It all starts with the vulnerabilities in your infrastructure. From 2019 to 2022, we saw a **466% increase in the vulnerabilities tied to ransomware.** This gives threat actors nearly 5x the attack surface to target. There are at least **250 ransomware families** in the wild, with just three or four typically responsible for most attacks--with dangerous new ones like LockBit, Hive, and Conti emerging all the time.

These attacks were accompanied by an **average of 19 days of downtime**. As an example of the potential damage, it is estimated that WannaCry ransomware has caused over **$4 billion in damage** to organizations in just a few short years.

Although the **remote desktop protocol** (RDP) was the primary attack vector for ransomware in the past, today, **email phishing** is the predominant method entry, accounting for half of all infections. Software vulnerabilities also continue to play an important role in enabling ransomware attacks.

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 pay a ransom.

HOW **SERIOUS A THREAT IS RANSOMWARE** TO YOU?

SOFTPROM

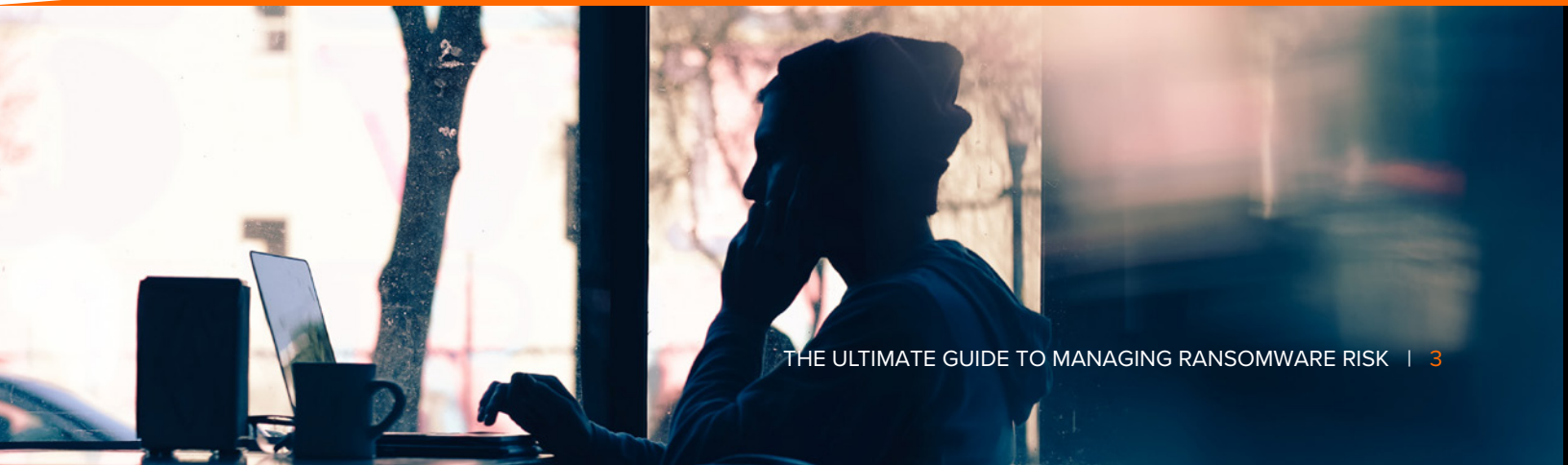
U.S. Deputy Attorney General Lisa Monaco has warned that U.S. businesses need to **prepare for a very large increase in the number of ransomware attacks** being made by criminal threat actors and hostile nation states or, in some cases, a blended collaborative threat of both. “The message…to the CEOs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

> There was a ransomware attack every 11 seconds in 2022—and those are just the ones we know about. For every known attack, as many as 30 others go unreported.

The recent cyberattacks on the Costa Rican government, the Colonial Pipeline, and the meat processing company JBS are reflective of the sorts of intrusions taking place every day. FBI Director Christopher Wray has noted that the attacks on Colonial Pipeline and JBS have parallels to the scale of challenges surrounding the terrorist attacks on 9/11.

Given the economics of ransomware, this problem will not go away soon. Director of the NSA and Head of U.S. Cyber Command General Paul Nakasone predicts **persistent ransomware threats “every single day” for the next five years**. Exploits of the Log4j RCE vulnerability, such as Log4Shell, are likely to have an impact here.

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



5 BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE ATTACKS

SOFTPROM

Fending off ransomware attacks calls for some common-sense best practices. They include (incomplete list):

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 a sophisticated 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. **TRAIN YOUR EMPLOYEES**
   Training your employees to be **aware of, recognize, and report email phishing attacks** is among the most important steps you can take. Make sure your protocols around identity verification are airtight. And as a final step, conducting a **social engineering "penetration test"** can help you validate that the training and protocol updates are working. (Bugcrowd offers all of the above through its partner, SocialProof Security.)

5 BEST PRACTICES FOR DEFENDING AGAINST RANSOMWARE ATTACKS

SOFTPROM

3. BACK UP YOUR DATA, SYSTEM IMAGES, AND CONFIGURATIONS; REGULARLY TEST BACKUPS; AND STORE BACKUPS SECURELY 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

Nothing 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?

HOW CROWDSOURCED SECURITY CAN HELP

SOFTPROM

In recent years, *crowdsourced security* has emerged as a way to content with the scale, complexity, and unpredictability of attacks from malicious hacker around the world. In this highly proactive approach to risk reduction, organizations engage with and incentivize third-party security researchers/ethical hackers to help them meet security goals--with discoverers of the most critical vulnerabilities receiving the highest rewards.

Although bug bounty and vulnerability disclosure programs were the original use cases for crowdsourced security, today, it also brings massive value to penetration testing, attack surface management, and more by utilizing an "attacker mindset" for defense, and by putting 10s, 100s, or 1000s of eyes on your vulnerabilities--with everyone competing to make the biggest positive impact.

In the context of ransomware, the crowdsourced approach can help you find hidden flaws before attackers do it first. Most orgs have no or limited visibility into their own "software supply chain", nor the access to skill sets needed to find them. A crowdsourced security program like a bug bounty or crowd-powered penetration test provides access to those skills on demand, so you stay ahead of ransomware gangs much more effectively than by relying only on reactive, noisy approaches like scanning.

RECOMMENDATIONS

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 open and exposed vulnerabilities.

If you would like to know more about accelerating ransomware risk management using crowdsourced security, Bugcrowd can help. Our Security Knowledge Platform™ matches you with the right trusted researchers at the right time, bringing them into security testing tasks "as a service"--handling all operational details, like triage, compliant payments, and reporting, for you.

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