

**mimecast**

**PART ONE**

# **Future- proofing your cybersecurity strategy**

Defending Against  
RANSOMWARE



## Ransomware Is Everywhere

Ransomware is running amok. The term refers to a type of malware that encrypts the victim's data, preventing the organization or individual user from accessing their files and records. In exchange for decrypting it, the perpetrator demands a ransom — hence the name.

According to recent reports:

- A ransomware attack occurs every 11 seconds,<sup>1</sup> and a staggering **84% of U.S. organizations** have reported phishing or ransomware attacks in the past 12 months.<sup>2</sup>
- Among businesses that operate globally, more than a third (**37%**) have been victimized by ransomware.<sup>3</sup>
- According to the FBI, the Internet Crime Complaint Center received **2,385 complaints** identified as ransomware in 2022, with adjusted losses of more than \$34.3 million.<sup>4</sup>
- One-third (**33%**) of cybersecurity decision-makers are thinking of leaving their role in the next two years due to stress or burnout.<sup>5</sup>

Those executives have good reason to worry. Analysts predict that the frequency of ransomware attacks will rise to one every two seconds,<sup>1</sup> as perpetrators refine their malware and attack methods. The cost of these attacks is expected to soar as well, reaching **\$265 billion by 2031**.<sup>1</sup>



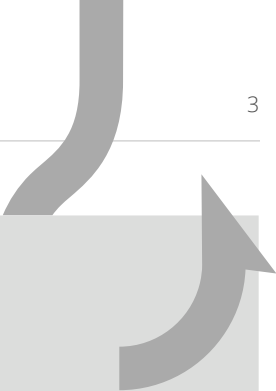
More than  
**1 out of 3**  
global businesses have  
been victimized by  
ransomware.

## Who Are the Victims?

Some of the world's most prominent businesses were the targets of ransomware last year. These ran the gamut from energy conglomerates to food processors to the National Basketball Association.


- **Colonial Pipeline**, for example, which supplies gasoline and jet fuel to the southeastern U.S., was forced to close down its entire pipeline network for five days owing to a ransomware attack.<sup>6</sup> It was the first time in its 57-year history that the company had to cease operations; and it was only able to resume them after paying a \$4.4 million ransom.
- Likewise, a ransomware attack last June forced **JBS Foods** to shutter all its beef processing plants in the U.S. To resume operations, the world's largest meat supplier was compelled to pay an \$11 million ransom.<sup>7</sup>
- **Acer**, the Taiwanese electronics and computer manufacturer, was hit by multiple ransomware attacks last year. Among them was a March 2021, attack demanding \$50 million in ransom<sup>8</sup> — the largest demand of its kind known to date.

Such incidents are no longer the exception — they've become the rule. Mimecast's *The State of Email Security 2022* report, based on an in-depth survey of 1,400 information technology and cybersecurity professionals from 12 countries, found that ransomware afflicted three-out-of-four (**76%**) companies worldwide in 2021, up from **61%** in 2020.



A ransomware  
attack occurs  
**every 11 seconds.**

Soon, one will  
take place  
**every 2 seconds.**<sup>1</sup>



## What Are the Consequences?

Measured in terms of downtime, the Mimecast study found that a quarter of the companies (**25%**) that suffered ransomware incidents experienced outages of **two-to-three days**, although nearly as many (**22%**) were down for a week, while another **15%** were dead in the water for up to two weeks.

The largest known ransomware payout to date was made by an insurance company for \$40 million. A survey of 1,263 companies found that although **46%** recovered their files after paying the ransom, most of the data was corrupted.<sup>9</sup> Meanwhile, **80%** of the victims that paid a ransom experienced another ransomware attack soon after.

## How Are Businesses Responding?

The sad reality is that when companies are confronted with a ransomware attack, nearly two-thirds (**64%**) feel compelled to pay off the attackers. Yet among companies that agree to pay a ransom, nearly four-out-of-10 (**39%**) fail to get back their data, according to Mimecast's *State of Email Security* survey. This begs the question: How *should* they respond? While it's easy to advise a company that it is self-defeating to pay off cybercriminals, the reality is not so simple. Companies must have access to their data to protect their customers and remain in business. Realistically, no company is in a position to defy its attackers — *unless it is thoroughly prepared to respond to a ransomware attack*.

Put another way, a ransomware attack is a declaration of war on a company, and for companies to wage a war successfully, they must have troops, weapons and a battle plan.



**4 out of 10**

companies that pay a ransom fail to get their data back.

## Defeating Ransomware: A Three-Part Approach

The battle against ransomware needs to be waged on three fronts:

### Securing Communications

As businesses have increasingly come to depend on email and other forms of electronic communications, new avenues of attack have opened up for cybercriminals. This has been particularly true since the start of the COVID-19 pandemic, when email use soared and companies turned to new collaboration tools like Microsoft Teams and Slack to replace in-person meetings. This swell of digital activity presented bad actors with numerous openings for social engineering attacks, many of which were devised to infect companies with ransomware.



To secure an organization's communications, it's critical to harden its business processes and infrastructure. This involves asking and answering many questions: Are your procedures stable and secure, or can they be ignored or manipulated? Do you frequently use software that can be easily exploited? Do you work with third parties whose security procedures and systems are less robust than your own? Once you begin to systematically explore these issues, you are likely to uncover numerous vulnerabilities that an interloper could use to gain access to your network.

### Securing People

Most successful cyberattacks succeed due to human error. Ergo, your top priority in the fight against ransomware should be to raise employee awareness and train them to recognize and respond to an attack. This is especially important since phishing is one of the most common methods used by cybercriminals to embed ransomware.



### Securing Data

Defending against ransomware amounts to an arms race. Perpetrators are quick to adopt the latest technologies in their efforts to encrypt and gain control of your data. An example of this are the malware kits that have become readily available on the dark web. These can be used even by those with minimal technical skills to quickly devise and disseminate new forms of ransomware.



This means that you, the defender, can't rely on yesterday's tech. Traditional ransomware detection tools can't keep pace with today's ransomware programs, and datanappers have found ways around conventional antivirus software. To secure your data and defend against incursions, you need specialized software that dynamically adapts to new threats.

## Mimecast: Your Best Ally for Ransomware Readiness

Mimecast offers AI-powered email threat protection, along with an array of robust tools and proven services, that can support your fight against ransomware on all three fronts. These let you:

- Email is the door through which most ransomware attacks enter your environment, and Mimecast Email Security can safeguard your organization against all forms of attack, including business email compromise. Comprised of multiple Mimecast and third-party detection engines and utilizing state-of-the-art machine learning, these targeted threat protection technologies guard against ransomware, phishing and an array of additional threats.
- Mimecast security awareness training was developed by leaders from the military, law enforcement and intelligence communities and will prepare your employees to detect and evade a ransomware threat. Utilizing humor and other engaging techniques, Mimecast training arms your troops with an understanding of the many ways that attackers may try to breach the company's security and the role they can play in disarming these attacks. For more on this, see our paper, *[Teaching Good Security Behaviors with Seinfeld: Overcoming the employee engagement challenge in security awareness training](#)*.
- Mimecast employs highly skilled cybersecurity professionals who can audit your IT infrastructure and business processes for potential security gaps and vulnerabilities. These experts will work with you to uncover any shortcomings in your systems and procedures, so you can correct any weaknesses before a datanapper can take advantage of them.
- If your network is infiltrated by malware, Mimecast's ransomware scanner will alert you to take the appropriate steps. These detection tools work by searching for key indicators of ransomware, such as particular file extensions, multiple file renames and certain unique codes. While it can't stop an attack once it's underway, the scanner will alert you when any abnormal behavior occurs on your network. This gives you a much better chance of halting a ransomware attack before your files are encrypted.
- Mimecast also offers other resources that help mitigate the consequences of a successful ransomware attack. These include an all-in-one subscription service for business continuity that enables your employees to continue to send and receive email even in the midst of a ransomware attack. Other services include email backup and recovery. Mimecast Sync & Recover, for example, rapidly restores mailboxes, calendar items and contacts lost through malicious deletion or file corruption, helping to minimize downtime and ensure a swift restoration of normal business operations.

## Conclusion: Seizing the High Ground

All of these Mimecast tools and services merit consideration for your ransomware arsenal. Deploying these defenses, together with a well-conceived battle plan and strong generalship from your CISO and their team of professionals, will fortify your organization against even the most pernicious ransomware attacks.

The war against ransomware will be a protracted struggle. But the defensive measures described here will allow you to seize the high ground from which to throw back the enemy's incursions.

---

<sup>1</sup> ["Global Ransomware Damage Costs Predicted To Exceed \\$265 Billion By 2031,"](#) Cybersecurity Ventures

<sup>2</sup> ["Osterman Research: How to Reduce the Risk of Phishing and Ransomware,"](#) Mimecast

<sup>3</sup> ["IDC's 2021 Ransomware Study: Where You Are Matters!"](#) IDC

<sup>4</sup> ["Internet Crime Report 2022,"](#) FBI

<sup>5</sup> ["The State of Ransomware Readiness 2022: Reducing the Personal and Business Cost,"](#) Mimecast

<sup>6</sup> ["Hackers Breached Colonial Pipeline Using Compromised Password,"](#) Bloomberg

<sup>7</sup> ["JBS Paid \\$11 Million to Resolve Ransomware Attack,"](#) The Wall Street Journal

<sup>8</sup> ["Computer giant Acer hit by \\$50 million ransomware attack,"](#) Bleeping Computer

<sup>9</sup> ["Ransomware: The True Cost to Business,"](#) Cybereason

# Work Protected.

Advanced Email & Collaboration Security

**mimecast**

[www.mimecast.com](http://www.mimecast.com) | ©2023 mimecast | All Rights Reserved | GL-4265-1

Mimecast is a cybersecurity provider that helps thousands of organizations worldwide make email safer, restore trust and bolster cyber resilience. Mimecast's expanded cloud suite enables organizations to implement a comprehensive cyber resilience strategy. From email and web security, archive and data protection, to awareness training, uptime assurance and more, Mimecast helps organizations stand strong in the face of cyberattacks, human error and technical failure.