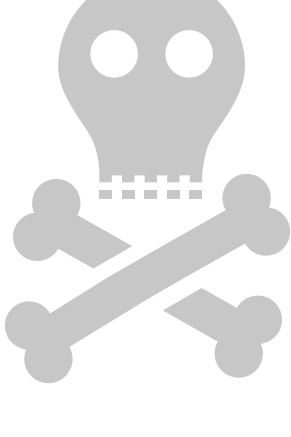




KONICA MINOLTA

# ARE YOU BEING HELD FOR RANSOM? FOR RANSOM?

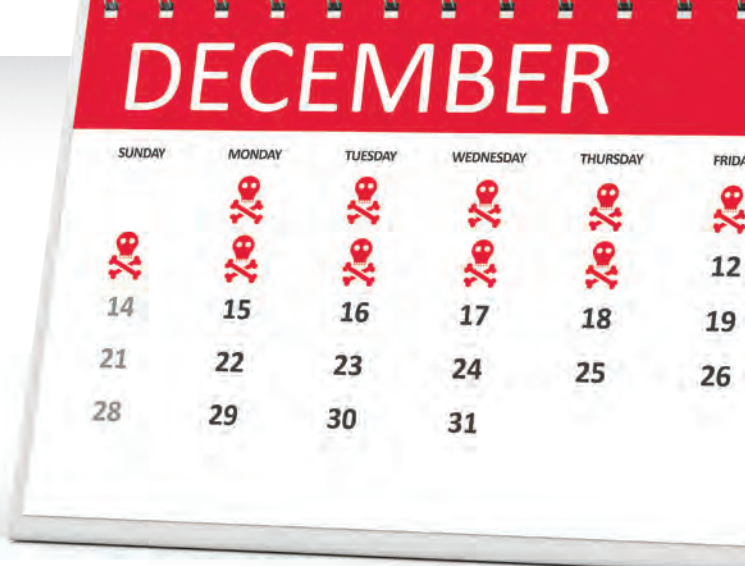


**Ransomware is a type of malware that restricts access to the infected computer system in some way and demands that the user pay a ransom to the malware operators to remove the restriction.**

Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.

## Ransomware plagues internet users daily.

Organizations are bombarded with attacks containing ransomware and their employees' lack of knowledge of what to do, unsuspecting users, and users in denial ("It won't happen to me.") can cause havoc with your corporate security.



Ransomware is the **fastest growing** security threat and is evolving.

Organizations of all sizes are being affected.<sup>1</sup>



**80%** of organizations see ransomware as an extreme to moderate threat.<sup>1</sup>

**40%** of ransomware infections increased in 2017 with a 46% increase in new infection variants. Some include cryptocurrency scams.<sup>2</sup>

**\$11.5 billion** is estimated in damage costs connected with ransomware in 2019.<sup>3</sup>

## United States

remains the most targeted country.<sup>2</sup>



**More than 50%** of organizations were hit with ransomware in 2017; most more than once.<sup>5</sup>

## 64% of Americans

are willing to pay a ransom after being victims of ransomware, compared to 34% globally.<sup>2</sup>



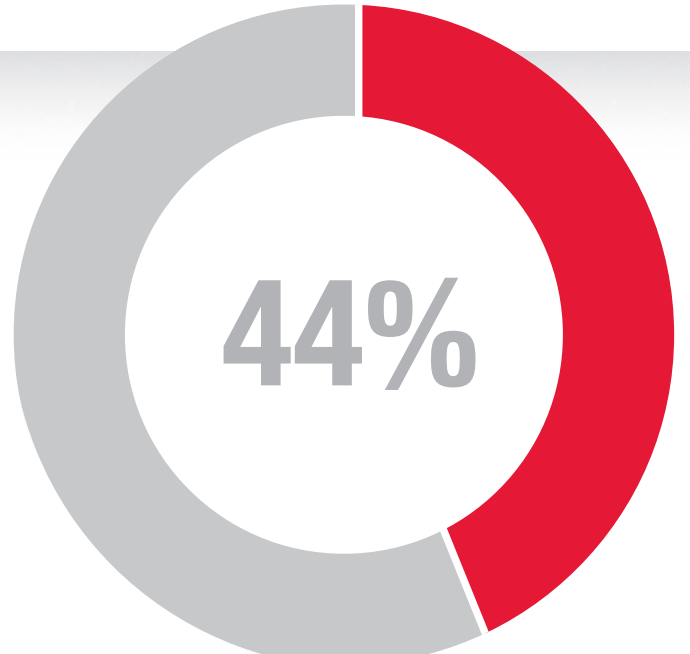
## Financial data,

followed by customer and employee personal information, and company IP are most at risk from attacks.<sup>1</sup>



## 44% of organizations

assess their probability as a ransomware target as very or extremely likely.<sup>1</sup>

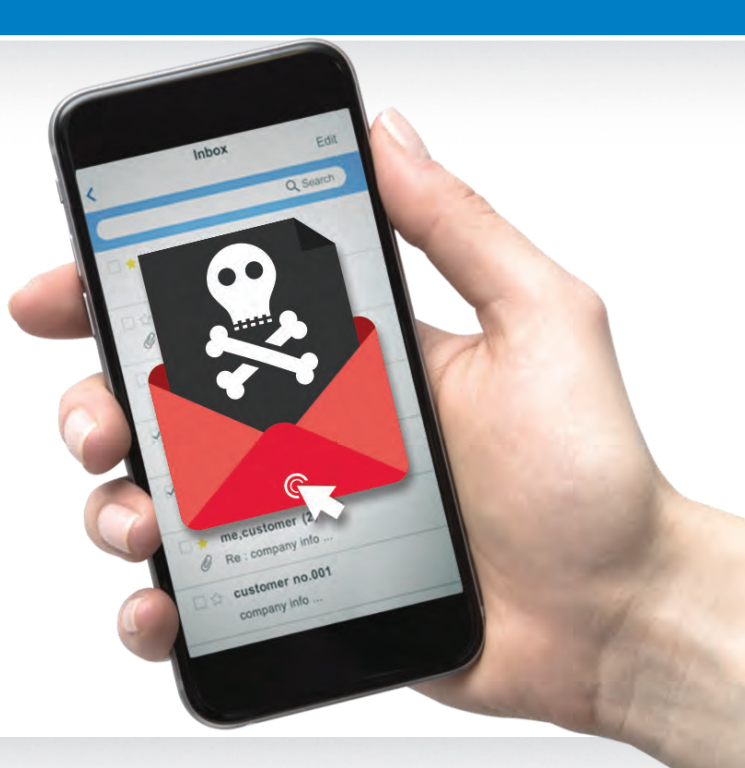


Ransomware impacts businesses, leading to negative consequences

which include system downtime, productivity loss, and data loss.<sup>1</sup>

## 92% of all malware

is delivered via email with ransomware being the most prevalent type.<sup>4</sup>



## Prevention is the cure.

Once your organization has opened the door, your IT team has to deal with the threat – but your information has been hijacked already. The best solution to protecting your organization is through prevention – by educating your security officers with a cyber security course of study, and communicating your corporate process to protect employees from falling victim.



**Konica Minolta can help.**

### Tools to Succeed:

Cyber Security Incident Response & Enterprise Cyber Security Program

### IT Services:

All Covered 

IT SERVICES FROM KONICA MINOLTA

#### SOURCES:

1. Bitdefender
2. Symantec
3. Cybersecurity Ventures
4. Verizon
5. Sophos