ransomware.org
understand · prevent · recover

POWERED BY ActualTech MEDIA

The State of Ransomware

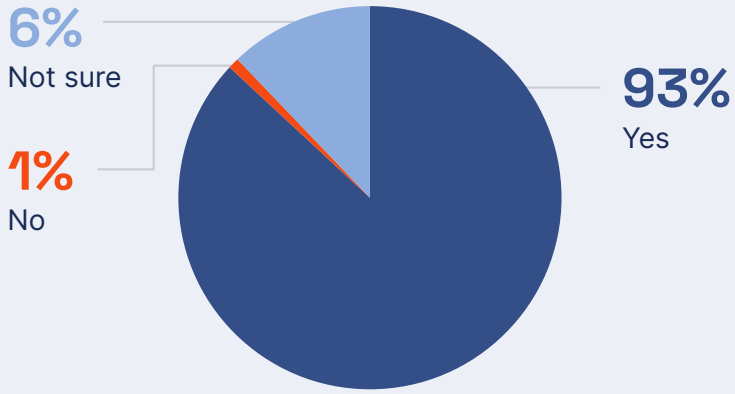
A REVEALING REPORT FOR IT PROFESSIONALS BY IT PROFESSIONALS

You may not have seen as many headlines for ransomware recently, but it is still out there. Like a lot of things, it becomes old news after a while and media companies move on to find the next big story. At some point people just accept bad news as a price of doing business. A quick web search however will confirm that ransomware is still rearing its ugly head for organizations the world over. From municipal government services to large corporate enterprises, from universities to small businesses, ransomware attacks continue to plague the networks of all types of organizations, and it continues to be a threat that keeps IT leaders up at night.

That's why we conducted multiple surveys involving IT and security professionals earlier this year to find out their perceptions of the current state of ransomware.

Ransomware attacks continue to plague the networks of all types of organizations.

Do you believe ransomware will continue to be a serious threat in 2023?



An overwhelming 93% of respondents agreed that ransomware will continue to be a threat in 2023.

(Image should show 211 out of 226). While ransomware may not be as prominent in the mainstream news, IT and security professionals still recognize it as a serious threat. Barely more than 1% stated they weren't sure of the risk level.

Why Ransomware Persists

Ransomware has been garnering headlines since 2013 when CryptoLocker first made a big splash in the world. CryptoLocker was the first of its kind, an advanced ransomware variant that used 2048-bit RSA encryption to make the files of a targeted victim unusable. It was also the first ransomware attack to use Bitcoin as its primary form of payment which made it easier for attackers to receive extortion payments anonymously. Like its descendants today, CryptoLocker was primarily distributed through email phishing attacks that use embedded links or infected attachments. CryptoLocker would bring in some $27 million over a nine-year period at which point it was brought down by law enforcement.

And yet, a decade later, ransomware persists today thanks to the lucrative business it has created for cybercriminals for multiple reasons.

Ransomware persists today thanks to the lucrative business it has created for cybercriminals for multiple reasons.

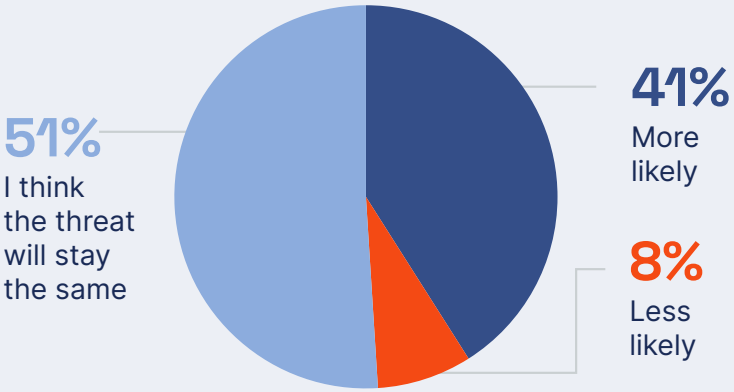
⚠ **Ransomware presents a low barrier of entry for malicious actors thanks to the Ransomware-as-a-Service" kits that are available for purchase by anyone willing to venture out into the abyss of the dark web.** Someone with minimal technical expertise can invest in ransomware software for a minimal fee plus a cut of any ransoms they may acquire. Many of these "as-a-Service offerings even include tech support and financial advisement as an added service.

- **For a business that requires such minimal investment, the potential payouts can be huge with the average ransom in 2022 being $2.2 million.** That amounts to a spectacular return on investment.
- **Ransomware has a vast target market.** Essentially, anyone with a computer is a potential target. In the era of digital transformation, that means that every organization is a potential victim.
- **Finally, ransomware is a low-risk crime.** Because ransomware attacks can be implemented from anywhere in the world, attribution is difficult due to the international jurisdictional challenges and anonymous ransom currency. All of this translates into low arrest rates for a highly prevalent crime.

Because of its low cost of entry, high payout potential and low risk of being apprehended, ransomware will continue to be a threat and IT and security professionals know it.

Anyone with a computer is a potential target. In the era of digital transformation, that means that every organization is a potential victim.

Compared to 2022, do you think your company is more or less likely to be a target of ransomware attacks this year?



Survey participants were asked if they felt their company was more or less likely to be a target of ransomware attacks in 2023.

A resounding 92% stated that the risk of an attack in 2023 would be the same or greater when compared to the year prior. Just over 40% think the chances will be greater. (The total 342 was used for these figures)

The Odds Favor the Bad Guys

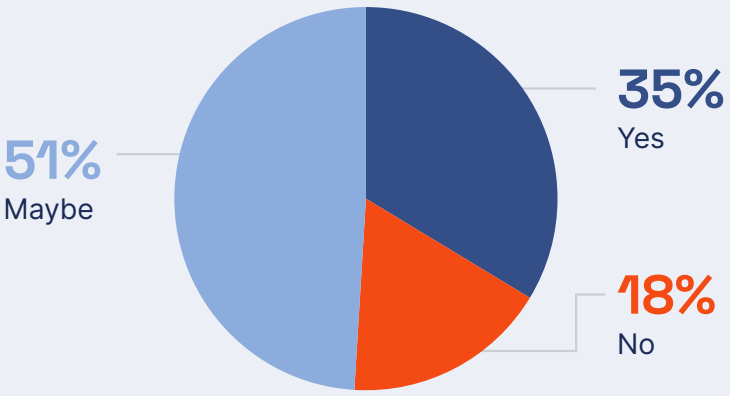
If your company has a network, then it has an attack surface. Ransomware criminals are committed to finding an exploitable vulnerability within that attack surface. It only takes one, and hardening every one of them is daunting.

If your company has a network, then it has an attack surface.

- **Ransomware targets unpatched vulnerabilities that reside in operating systems, Exchange servers and software applications.** Patching and updating is a perpetual process that creates little value for a business other than mitigating an exploit.
- **Organizations must have a modernized email security system** that can block email from known malicious sites, strip embedded links and attachments deemed malicious and use intelligent driven policies to identify suspicious identities about any email.
- **IT admins must secure the web browsing sessions of company users** as threat actors deposit malicious code on malware distributable websites and in some cases, even legitimate sites.
- **The remote work movement has created great opportunities for hackers** that know how to exploit weak RDP credentials to gain access to a corporate network and launch an attack.

IT and cybersecurity professionals are aware of the sizable disadvantage they have out of the gate in preventing a ransomware attack.

Do you believe your organization is ready for a ransomware attack?



According to our survey, only 1 in 3 respondents said that their organizations were ready for a ransomware attack.

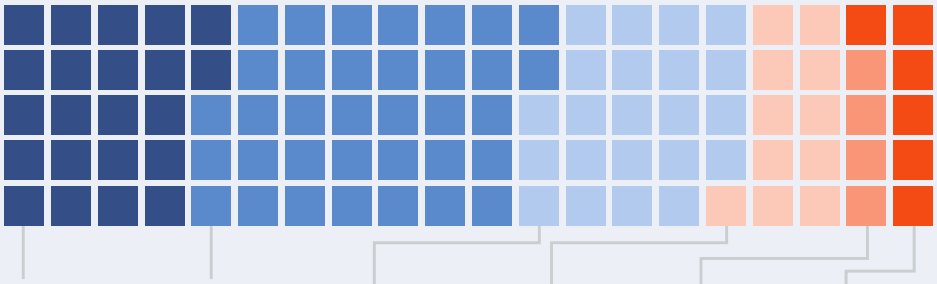
Just less than half were unsure and only 18% resoundingly said yes. (These figures were based on a total of 255).

Public Awareness of Ransomware

Because of highly publicized incidents in 2021 such as The Colonial Pipeline and Kaseya, ransomware is known to people other than in the IT field. They may not know what it is or how it is deployed, but they know it its disruption to business.

The IT and security professionals who participated in our survey were asked if they felt other members of their organization were aware of the potential threat of ransomware.

Do you think those in your organization are well aware of the threat?



22%	35%	22%	11%	4%	2%
Very well aware	Most are aware	It's 50/50	Few are aware	Almost nobody cares	No awareness whatsoever

Recovering from an Attack

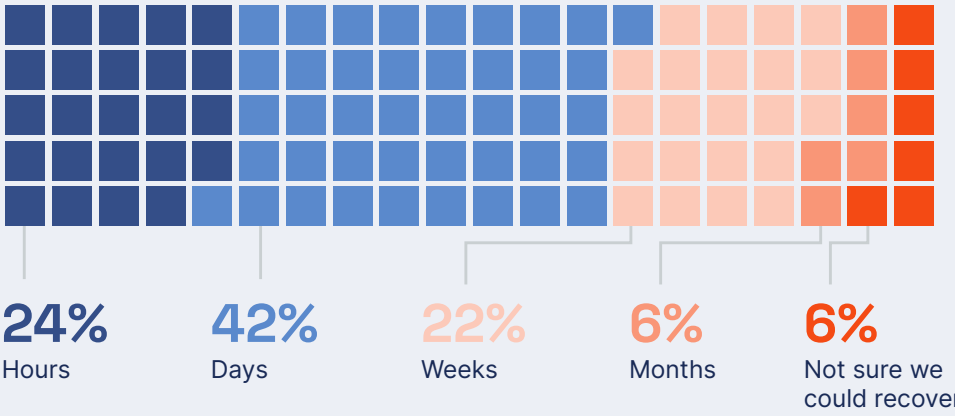
No one wants to pay a ransom to malicious criminals, yet for many organizations, the cost of remediation can end up being significantly greater than the ransom itself. Some of the endured costs include the cost of outside security and forensic specialists, overtime pay, legal fees, increased security measures, litigation costs and damages. One of the biggest costs, however, can be lost revenue. When your business operations are shut down, so is your money intake. There is also historical evidence that a company's stock price can be impacted by a severe ransomware attack. How a company responds to a cyberattack can have a direct impact on their reputation or company brand. Reputational damage can haunt a company financially long after an attack.

How a company responds to a cyberattack can have a direct impact on their reputation or company brand.

Rapid recovery is an essential ransomware objective for any organization. That's why it is imperative to have a well-rehearsed incident response plan that can be immediately set into motion once an attack has been detected. You can have all the best-of-breed security tools available, but they will prove ineffective without a response team that knows how to work in coordination with one another.

We finished out our survey by asking our IT and security respondents which time measurement was most appropriate for estimating the length of time it would take their company to bounce back from a ransomware attack.

How long would you estimate it would take for your organization to bounce back from a ransomware attack?



Conclusion

While ransomware may not be at the top of the headlines for right now, it should be at your top-of-mind awareness (TOMA) when it comes to securing your network. While zero-trust security may be realistically unobtainable for many organizations, there are proven strategies today that can your risk to ransomware attacks and contain them once identified so that they don't spread. There are also new technologies and security controls that allow companies to recover quickly and avoid the costly duration of downtime. The threat of ransomware may be a fact of life for now, but it doesn't have to be a cost of doing business.

Want more ransomware information? Visit ransomware.org >