THINK YOUR CUSTOMERS WILL FORGIVE A RANSOMWARE ATTACK? THINK AGAIN.

Every day, cyberattacks bring organizations like yours to their knees—and the repercussions stretch far beyond the immediate impact on your IT department. Damaging news coverage. Shaken confidence in your leadership. Idle employees. Costly non-compliance penalties.

Realizing there was more to the story, we surveyed nearly 2,000 consumers across North America, the U.K., France, and Germany. What did our research reveal? In short, ransomware also deals a devastating blow to consumer loyalty and purchasing behavior.

Do you value...

Consumer trust?

70% don't believe businesses today are doing enough to secure their data

93% question if they can trust your business before making a purchase

Your reputation?

84% have shared their negative, ransomware-related experiences online, by email, and with the people in their lives

19% admitted to viewing your business as incompetent after experiencing a ransomware attack

Supporting business growth?

39% said the sole reason they opted not to open an account or make a purchase was out of concern for their data security

59% are so protective of their data that one ransomware attack in the past year is concerning enough to keep them from doing business with you

Meeting SLAs?

28% said they'd walk away if they were unable to access information, complete a transaction, or encountered a service disruption on just one occasion - and that skyrockets to 58% with two or fewer disruptions

37% said they'd switch to a competitor if your systems and applications aren't back online within 24 hours

You're more vulnerable than you realize

Organizations just like yours have data protection and security in place—but those solutions are often siloed and woefully inadequate. And, in the face of new threats—from natural disasters to COVID-19 to disgruntled employees—cybercriminals are seizing upon the opportunity to profit from your pain.

In fact, they did just that last year—successfully targeting 78% of organizations, according to CyberEdge Group.

Munson Healthcare Group patient data accessed for **2-1/2 months**

Travelex hit with a **$6M USD** ransom demand—IT systems offline for more than 3 weeks

MGM Resorts data breach compromised the personal data of **$10M guests**

> "Cybercriminals are like looters—they see opportunity in chaos, and the gloves are coming off. That's because they know organizations will not only feel greater pressure to pay ransoms—but pay them more quickly, too. I expect 80% of companies are going to be hit by a ransomware attack this year."
>
> *- Sam Roguine, Arcserve Director of Solution Marketing & Enablement*

The good news—ransomware protection is great for business

Consumers take their data security seriously.

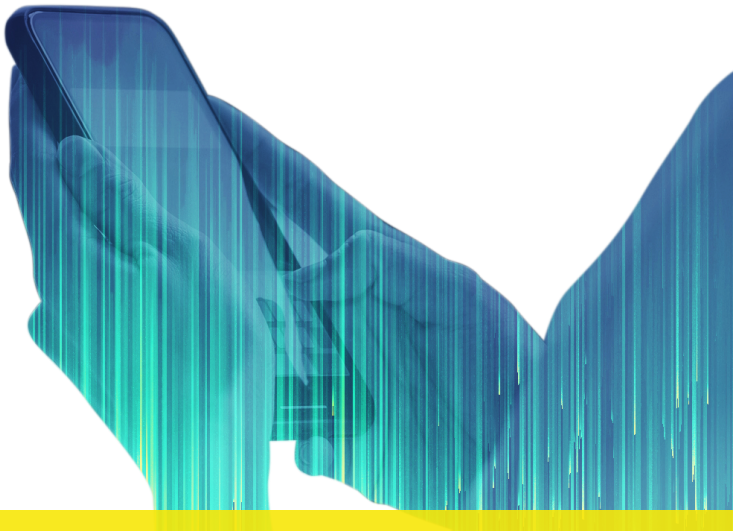
So much so, in fact, that 43% are willing to pay more for products and services across all sectors if the company can deliver peace of mind—and that figure goes up to 51% for banking and security businesses.

Protect consumer data—and your bottom line—with Arcserve

Consumers have spoken loud-and-clear—they simply won't tolerate service disruptions or breaches of their personal data. In fact, all it takes is the perception that you're not adequately protecting their data to keep them away.

Earn their trust. Retain their business. Deliver on expectations.

With Arcserve solutions secured by Sophos, you'll protect your critical consumer data with all-in-one threat prevention, backup, and disaster recovery technologies for on-premises, cloud, and SaaS cloud data.



Find out how you can simplify your data protection and security.

+1 844 639-6792
arcserve.com