Ransomware

arcserve®

RANSOMWARE'S STUNNING IMPACT ON CONSUMER LOYALTY AND PURCHASING BEHAVIOR

If you think your business is immune, think again. Recent research reveals consumers aren't as forgiving as you might think.

Discover how quickly they'll say enough is enough—and walk away.

Table of contents

About this research 2
Key discoveries... 3
Ransomware is an IT menace 4
Ransomware attacks will decimate your bottom line........................... 5
When you're down—consumers will take their business elsewhere 6
Consumers aren't shy about voicing their frustrations............................... 7
Protecting consumer data from ransomware can boost your bottom line 8
To drive buy-in, connect ransomware and data protection to your organization's bottom line............... 9
Arcserve solutions secured by Sophos....... 10

ABOUT THIS RESEARCH

Cyberattacks have crippled organizations. The media has widely reported their devastating impacts and, today, most within the IT community understand what's at stake. What's not understood, however—and what organizations rarely discuss or consider—are the quantifiable short- and long-term impacts of ransomware attacks on consumer purchasing behavior and brand loyalty.

In the aftermath of a cyberattack, when will consumers say enough is enough? At what point will they seek out a competitive product or service? We surveyed 1,998 consumers across North America, the UK, France, and Germany to find out.

About our survey respondents

More than half of our survey respondents transact business online—with three-quarters leveraging accounts for online banking and nearly 80% for digital communications. Interestingly, not only are a majority aware of data security threats, but they're also actively engaged in data protection best practices. They're using antivirus software, installing updates, and using two-factor authentication, as well as keeping passwords private and periodically changing them.

Are organizations holding up their end of the bargain? Consumers don't seem to think so. Nearly 70% of survey respondents believe businesses aren't doing enough to adequately secure their information, and they assume their data has been compromised without them knowing it.

This should come as a stark warning for business and IT leaders alike, particularly given that nearly nine of ten respondents consider the trustworthiness of an organization before purchasing a product or service.

How many customers are you potentially losing?

KEY DISCOVERIES

The consumers we surveyed made it abundantly clear: If you fail to protect their data from ransomware attacks or ensure access to information—even once—they'll exit stage-right for a competitor that can.

70%

of survey respondents believe businesses aren't doing enough to adequately secure their information—and they assume their data has been compromised without them knowing it

39%

said security concerns about their personally identifiable information (PII) was *the sole reason* they chose not to open an account or transact with a business

93%

consider the trustworthiness of an organization prior to purchasing

59%

shared they would likely avoid doing business with an organization that experienced a cyberattack in the past year—and that their level of forgiveness won't increase much with time

28%

said they'd take their business to a competitor if they encountered even a single service disruption, failed transaction, or instance of inaccessible information—with nearly 60% saying it would only take two or fewer disruptions or failed transactions

84%

admit to sharing their negative, ransomware-related experiences with family, friends or colleagues, posting about their experiences online, or emailing about the incidents

43%

said their data security is so important they'd be willing to pay more for products and services from an organization they believe to be reliable and secure—with many industries seeing that percentage rocket to 50% or more

RANSOMWARE IS AN IT MENACE

Like looters stripping stores of their big-screen TVs amid mass chaos, cybercriminals take advantage of major disruptions—and hold organizations hostage when they're most vulnerable.

Are you prepared? Many are not.

Faced with threats that run the gamut—from COVID-19 and massive wildfires to hurricanes and run-of-the-mill disgruntled employees—organizations are experiencing systemic failures with ever-increasing frequency.

The severity and frequency of ransomware attacks will rise

In 2019, 78% of organizations just like yours fell victim to a successful ransomware attack, according to CyberEdge Group. We expect the ferocity of these attacks to increase. Why?

Organizations often take a piecemeal approach to their data protection and security. And, in the wake of rushed transformation, fragmented environments—patched together over years—reveal weaknesses. What's more, every remote computer becomes a new data center you must protect. And, unattended machines left empty by remote workers become prime targets for cryptomining. Amidst the chaos and confusion, advanced data security, backup, and disaster recovery (DR) are often left behind.

Gaps become rampant.

And, if there's one thing you can be sure of, it's this: Cybercriminals will seize the opportunity in your organization's vulnerabilities. They'll multiply your pain—and profit from it.

People are more likely than ever to fall for cybercriminals' tricks

People's willpower naturally runs low as the workday progresses, according to Dr. Kathleen Vohs. And, in the face of disasters—natural, human-caused, or digital—they're exhausted. They're emotional. Their "immune response" to phishing attacks and drive-by downloads gets progressively weaker.

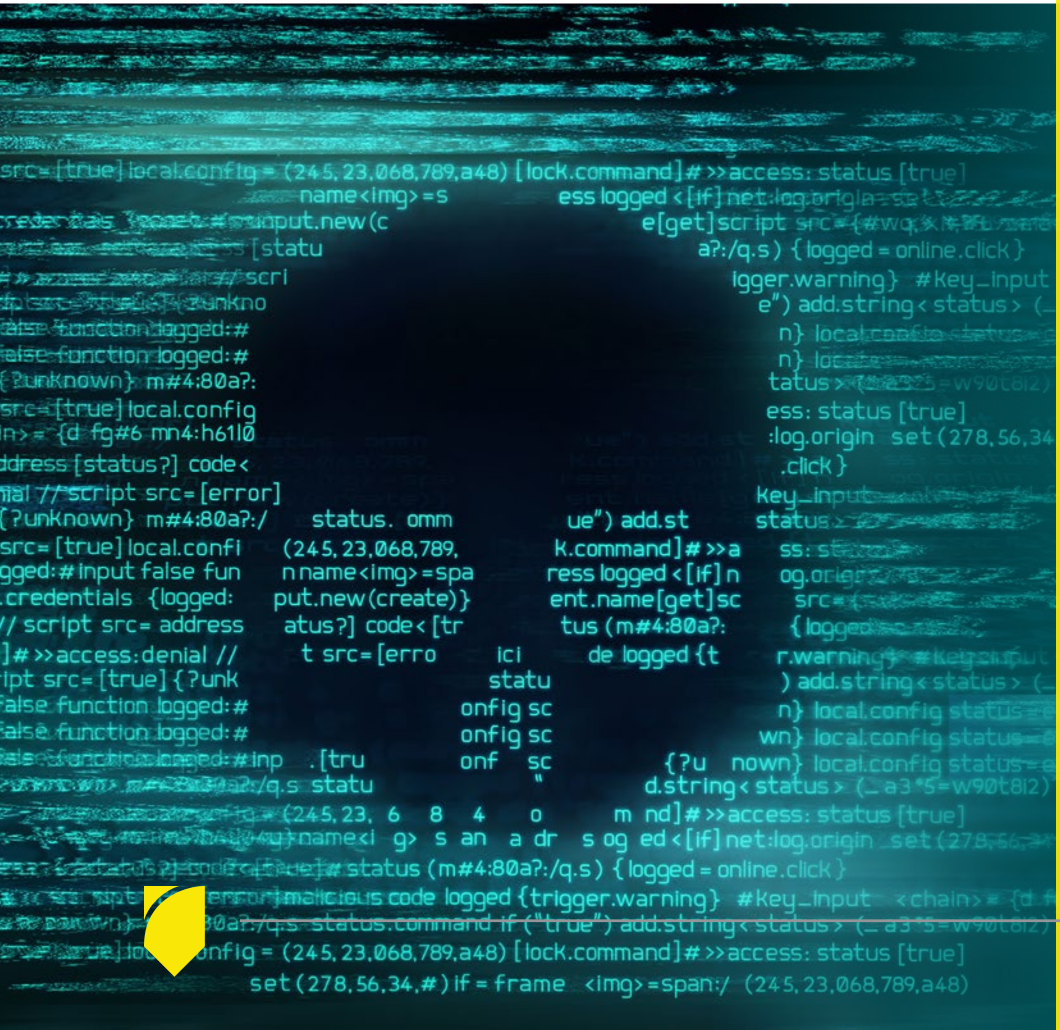
In search of critical information and motivated by altruism, they'll open files, click links, and transfer data and money they would have avoided under normal circumstances.

Your work has never been more critical.

RANSOMWARE ATTACKS WILL DECIMATE YOUR BOTTOM LINE

Consumers, driven by their desire for instant gratification, are increasingly transacting business online. But, they're wary. In fact, nearly three-quarters of the consumers we surveyed told us they didn't believe organizations were adequately protecting their data.

These concerns will drive their business to you—or your competition.



When it comes to businesses that can't protect data—consumers are unforgiving

93%

consider whether your organization or website is trustworthy before choosing to do business with you

39%

cite security concerns *as the sole reason* they haven't done business with an organization

59%

are likely to avoid doing business with you if you've experienced a cyberattack in the past year

45%

won't do business with you if cybercriminals have attacked you in the past three years—proving bad memories linger

You can't keep ransomware attacks quiet—not anymore

There was a time when organizations could pay the ransom and keep a cyberattack under wraps. No longer. Cybercriminals are now making breaches public—even when ransoms are paid.

Given how important trust and data security are to consumer preferences, ask yourself: Are you doing all you can to earn their loyalty?

WHEN YOU'RE DOWN—CONSUMERS WILL TAKE THEIR BUSINESS ELSEWHERE

If your organization experiences ransomware-related downtime, consider one out of every four of your consumers gone. That's because, in today's on-demand economy, a single service disruption, failed transaction, or instance of inaccessible information feels like a lifetime.

It's this intolerance for service disruptions that is, arguably, the most devastating impact of ransomware uncovered by our survey. And, the consequences stretch far beyond the immediate aftermath of an attack.

Consumers won't tolerate ransomware-related service disruptions

58% will switch to a competitor if they experience two or fewer disruptions

28% will walk away after just one disruption

46% will walk away from their banking or securities company after a single disruption

45% will walk away from a retail outlet after a single disruption

43% will walk away from their communications and insurance providers after a single disruption

Consumers won't wait for your ransomware recovery

In the aftermath of a cyberattack, many organizations bring operations to a halt—taking systems and applications offline while they assess the damage and recover backup data. But for many consumers, time is really of the essence.

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

41% will walk away if they can't access systems and applications within two to three days

49% will switch to a competitor if their banking or securities systems and applications aren't back online within 24 hours

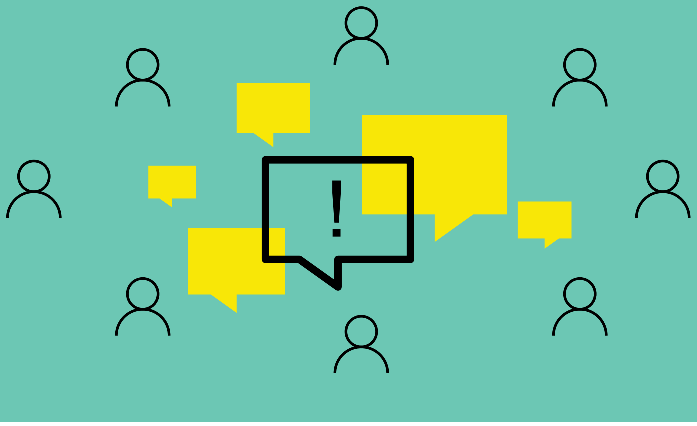
45% will switch their communications product or service if they don't have access within 24 hours

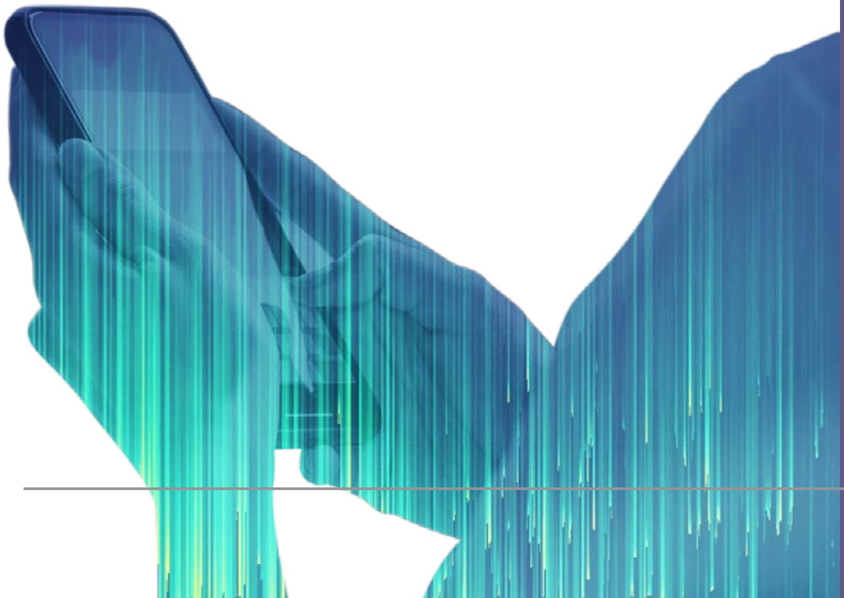
16% will walk away from their banking, securities, or communications businesses immediately

CONSUMERS AREN'T SHY ABOUT VOICING THEIR FRUSTRATIONS

The residual impact of cyberattacks may shock you. In fact, the majority of consumers have shared their past experiences of ransomware with family, friends, and colleagues—and a quarter have broadcast their experiences online.

In short, an unhappy consumer is also a vocal one. So, if you fall victim to a cyberattack, prepare for a deluge of bad news.





Consumers are vocal about their ransomware-related experiences

45%
have shared negative experiences with family, friends, or colleagues

25%
have posted experiences to a community forum, blog, or website

24%
have shared experiences via email

23%
have posted negative online reviews or shared experiences on social media

Get your public relations engine ready

28%
will see you as less trustworthy and reliable

24%
will think you're not spending enough on security

17%
will believe you're incompetent—more concerned with your profits than their security

PROTECTING CONSUMER DATA FROM RANSOMWARE CAN BOOST YOUR BOTTOM LINE

Cyberattacks weigh heavily on consumers as they consider purchasing decisions, but our survey did reveal some good news—ransomware protection is truly great for business. In fact, **more than four out of every 10 consumers would be willing to pay *more* for products and services if they believe you can reliably secure their data.** And, that figure **jumps to five in 10 or more for some industries, like banking and securities.**

Could you actually charge more for your products and services?

43%

will spend more—across the board—for products and services from a business they consider to be more reliable and secure

51%

will pay more with banking and security businesses

44%

will pay more with communications, data storage, and public cloud providers

39%

will pay more with media services, education, and transportation organizations

43%

will chip in more for government services

45%

will spend more for healthcare and insurance services

42%

will pay more for utilities

41%

will pay more for retail purchases

TO DRIVE BUY-IN, CONNECT RANSOMWARE AND DATA PROTECTION TO YOUR ORGANIZATION'S BOTTOM LINE

You feel the pressure. You know you're responsible for protecting the lifeblood of your organization—*its data*—and you know you're not fully equipped. How do you help decision-makers see beyond the sticker price of data and ransomware protection and, instead, consider its value to the business?

✓ **Help decision-makers gain a crystal clear picture of your organization's ransomware risk.**
Let them know cybercriminals successfully targeted 78% of organizations with ransomware last year—and highlight recent industry examples to tell a compelling story (see on the right).

✓ **Steer clear of nitty-gritty technical details—focus instead on immediate business continuity impacts.**
Walk-in ready to share how much your company will lose if it's down for a minute, an hour, a day, or a week. Communicate bottom-line impacts, like potential ransom demands, lost data and revenue, unwanted news coverage, regulatory fines, and idle employee time.

✓ **Paint a picture of ransomware's immediate and long-term impacts on consumer loyalty and purchasing decisions.**
Calculate, for example, the bottom-line impact to your business if 28% of your customers walked away following a single ransomware-related service disruption.

✓ **Demonstrate that ransomware protection can be a competitive advantage.**
Consumers value the security of their data. Make sure decision-makers understand they're also willing to pay more if you can deliver peace of mind.

✓ **Get decision-makers excited about the brand, not the product.**
Most don't care about features and technical specs. What they do care about is the strength of a brand's reputation.

✓ **Share our one-pager, "Think your consumers will forgive a ransomware attack?"**
This high-level overview delivers the fresh, much-needed perspective that's critical to your decision-makers' calculus.

✓ **Kick-off the conversation with your director of IT or your CIO.**
By getting a tech-savvy advocate on board early, you'll have an ally who can help shift the conversation from the cost of investment to the value to your business.

Ransomware stories like these can help highlight the need for urgent action

MUNSON HEALTHCARE

When 29 employees of this northern Michigan healthcare organization fell victim to a phishing campaign, cybercriminals quietly gained access to patient data for two-and-a-half months—including treatment information, banking information, and social security numbers.

Travelex worldwide money

Following a REvil attack, cybercriminals not only demanded $6 million USD from the UK financial institution, but they also claimed they had consumers' personal and credit card data. Travelex took its IT systems and websites offline for more than three weeks under the guise of "planned maintenance."

MGM RESORTS INTERNATIONAL®

Ransomware attackers gained access to the hotel chain's cloud server and the personal data of more than 10 million of its guests—including pop singer, Justin Bieber, and Twitter CEO Jack Dorsey.

ARCSERVE SOLUTIONS SECURED BY SOPHOS

You know your customers won't tolerate ransomware-related downtime or data security breaches. So, turn to Arcserve.

Leveraging fully integrated Sophos technologies, we deliver you complete protection from cyberattacks, major disasters, human error, and other unplanned outages. Trust the experts—leverage the only proven solution set designed by vendors with over 70 years of combined experience.

- ✓ Achieve IT resilience faster by eliminating the juggling act of multiple vendors, SLAs, and support teams
- ✓ Get total SaaS-based, on-premises, and cloud data protection from one vendor with unified backup, cybersecurity, DR, and cloud services
- ✓ Keep operations running and meet SLAs with instant VM and bare-metal restore (BMR), local and remote virtual standby, application-consistent backup and granular restore, hardware snapshot support, and extensions delivering high availability and tape support
- ✓ Ensure you don't miss a beat during on-premises outages with remote virtual standby for emergency failover and failback to the cloud, manually triggered failover to remote resources, and instant VM recovery
- ✓ Eliminate headaches from intentional or unintentional deletion, programmatic issues, external security threats—issues not covered by Microsoft—with total data protection for Exchange Online, OneDrive for Business, and SharePoint Online
- ✓ Detect known and unknown malware without relying on signatures, thanks to fully integrated Sophos Intercept X Advanced with cutting-edge deep learning technologies (AI)
- ✓ Prevent major hacking techniques, including credential harvesting, lateral movement, and privilege escalation with exploit prevention
- ✓ Stop ransomware attacks on backup data with CryptoGuard, and master boot record attacks with WipeGuard
- ✓ Ensure compliance mandates are met with AES encryption and role-based access control
- ✓ Keep up with data growth by dramatically reducing storage requirements with built-in global deduplication that frees up to 20X more capacity

NEED SUPPORT?

Count on Arcserve. We're always standing by—we're always ready to roll up our sleeves and lend a helping hand.

arcserve®

+1 844 639-6792
arcserve.com

This document is for your informational purposes only. Arcserve assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, Arcserve provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will Arcserve be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill or lost data, even if Arcserve is expressly advised in advance of the possibility of such damage. AD200063