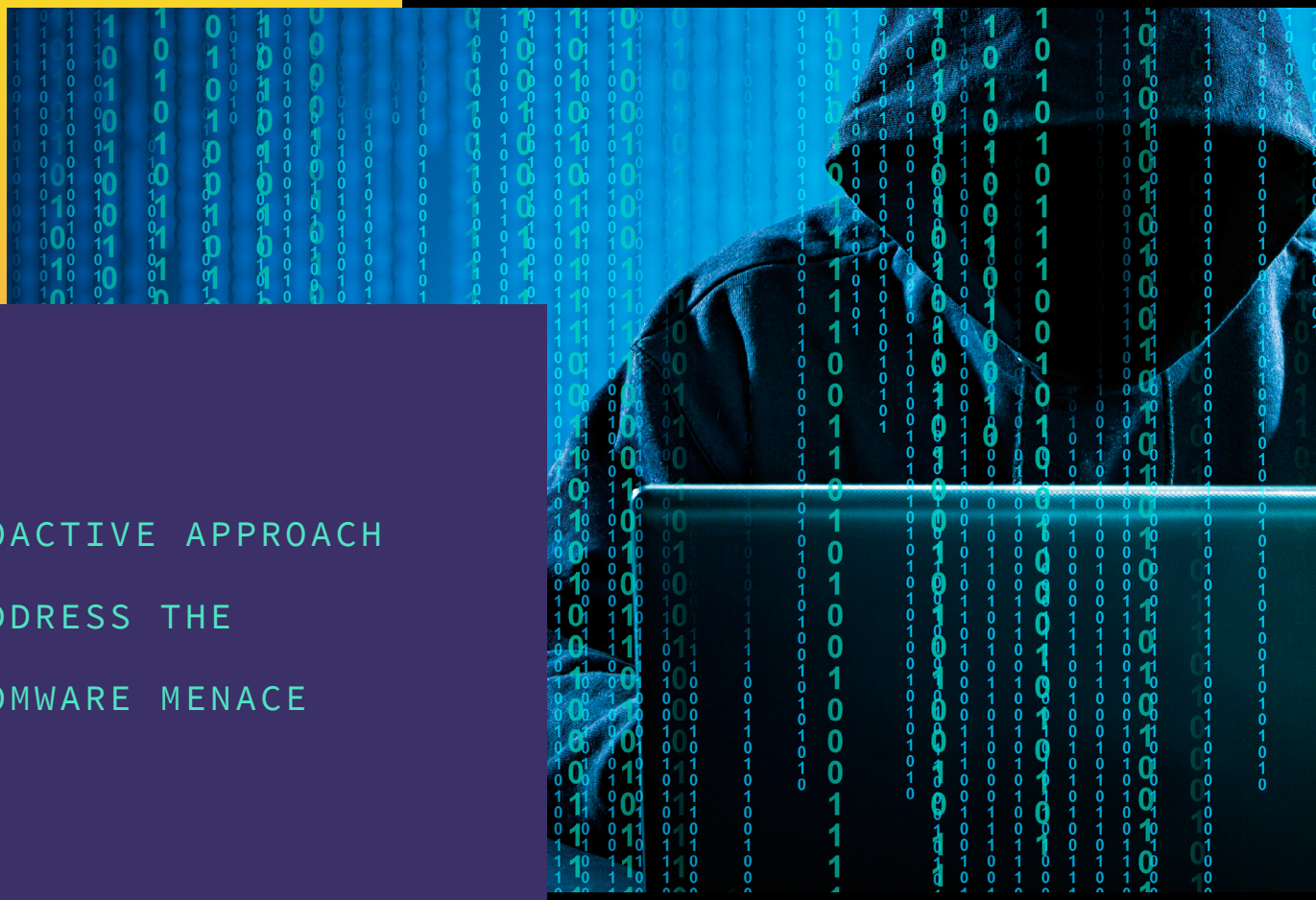
arcserve®

Protect what's priceless.

YOUR GUIDE TO A RANSOMWARE-FREE FUTURE



A PROACTIVE APPROACH TO ADDRESS THE RANSOMWARE MENACE

WHITE PAPER

RANSOMWARE HAS BECOME ONE OF THE LARGEST BUSINESS RISKS AND SERVES AS THE MOST MENACING THREAT TO IT ORGANIZATIONS.

Ransomware has become one of the largest business risks and serves as the most menacing threat to IT organizations. It's reached epidemic proportions globally, with costs projected to reach $20 billion by 2021.[1]

Yet, for IT professionals and business decision makers, the news doesn't need to be dire. While cyber criminals are showing no signs of slowing down, advancements in anti-cybercrime and disaster recovery technologies combined with sound IT management practices let organizations fight back.

This report explores the evolving threat of ransomware, the technologies and IT management practices being used in defense, and a forward-looking approach to realizing a ransomware-free future.

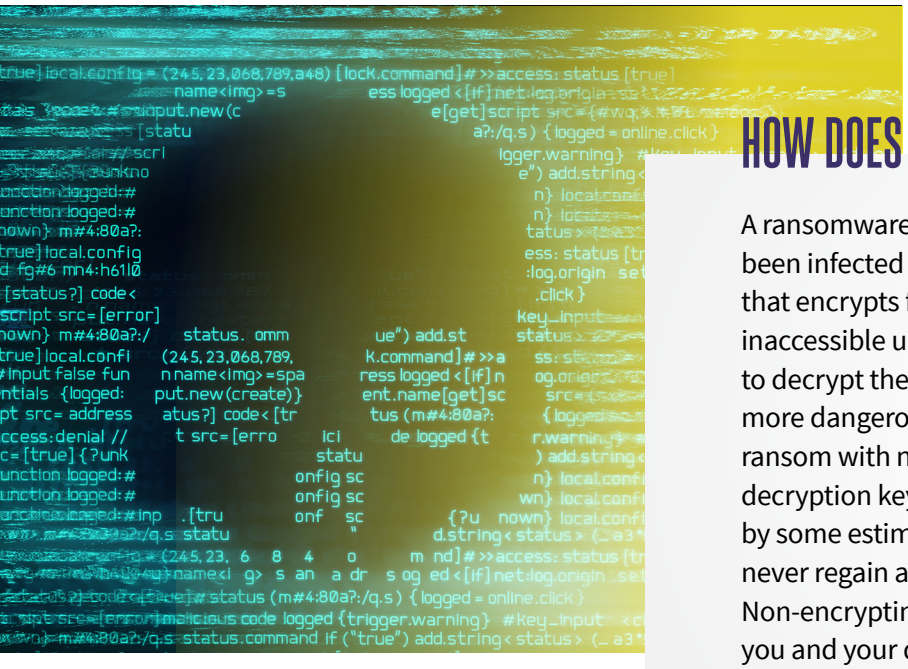
KNOW THE ENEMY

The Chinese military strategist Sun Tzu wisely advised "Know your enemy." To develop a strategy to secure IT systems from ransomware, you must understand it. Therefore, let's begin by exploring what ransomware is.

Data is the lifeblood of your organization. It represents your operations as it flows between business units. It tracks the past, communicates the current state of business and drives decisions. Without it, it's not a stretch to say that you have no business. And that's the idea that ransomware capitalizes upon.

Ransomware is a malicious software designed to deny access to your computer systems or data until a ransom is paid. It can stop your business dead in its tracks, or, if it is also leakware or extortionware, it can go a step further and threaten to exfiltrate and expose your data.

Any organization with important data stored on computers or networks is at risk -- which these days is just about every organization. State and local governments, law enforcement agencies, healthcare organizations, banks and credit card companies are all big targets, with the identity theft industry fueling the market by stealing a reported $14.7 billion from consumers in 2018.[2] It is not just large organizations that are affected either; ransomware attacks happen to consumers and corporations, small and large organizations alike.



HOW DOES RANSOMWARE WORK?

A ransomware attack takes place when a computer has been infected with a virus. Most ransomware is cryptoware that encrypts files on the affected computer, making files inaccessible until a ransom is paid in exchange for a key to decrypt the files. But be careful what you pay for. Even more dangerous, fake crypto encrypts files and demands ransom with no subsequent exchange of a working decryption key. Victims of this kind of ransomware, which, by some estimates, accounts for around 50% of cases, may never regain access to their files, even after paying ransom. Non-encrypting ransomware places a lock screen between you and your data, without directly encrypting it.

Ransomware can attack specific files, or the entire system via the Master Boot Record (MBR) of a drive or Microsoft's NTFS, thereby preventing the operating system from booting up. Ransomware often avoids detection by using a network such as HTTPS encrypted traffic or Tor. Unlike other kinds of malware which may operate in the background, once ransomware has infiltrated the unfortunate host, it will make its presence known while demanding untraceable cryptocurrencies for ransom payment.

It can take just one small, inadvertent action by an innocent user—such as clicking on a malicious link--for a computer to become infected. Ransomware typically spreads through phishing emails, but cyber criminals use numerous techniques to infect victims with ransomware. Infection generally occurs after opening an email attachment or clicking a deceptive link. Common vectors used to disseminate malware include:

Emails and text messages containing links that will download malware or an attachment containing malware

Websites whose sole purpose is to draw in users and get them to click on a malicious link or a download

Malvertising or malicious advertisements that are essentially click-tricks leading to unintended downloads

Social media that may seem connected to trusted sources, but quickly leads to a devious cybercriminal. Unwitting victims pick up the infection directly within a social media application or may be drawn to a malicious link or advertisement.

Mobile apps users willingly download to their device, not realizing they are actually fake and designed to transfer a virus the next time the mobile device is connected to a computer.

Hackers are becoming more sophisticated, targeting users by sending infected attachments in an email seeming to be from someone in their contact list. And while usage policies and training are helpful to reduce risky behavior by end users, it's impossible to completely eliminate this vulnerability as entry points may not always be so obvious. Malicious content may exploit vulnerabilities in the browser or plugins and run malicious code without the user's knowledge. Once established on a host, an infection can spread easily to other computers on the same network.

Beyond baiting users to unknowingly download ransomware, cyber criminals gain access to systems over the internet while no one is around. They use both brute-force methods and credentials purchased on the dark web to gain access to resources and data, leveraging Remote Desktop Protocol and software vulnerabilities

A 2019 report revealed that among enterprises and government organizations, the most common targets for ransomware are high-value assets such as servers, application infrastructure, and collaboration tools. While IT organizations may rightly prioritize the trending and most critical vulnerabilities first, older or less critical ones cannot be ignored. In the report, older vulnerabilities (those three years or older) accounted for more than one-third of attacks, more than half of which preyed on the less critical vulnerabilities.[3]

RANSOMWARE ATTACKS ON AVERAGE CAUSE NEARLY 10 DAYS OF DOWNTIME.[4]

What are the impacts of a ransomware infection?

Continuous ransomware news stories about attacks and an onslaught of frightening statistics have already prompted companies to take notice and look for data security or data protection solutions that work. The immediate effect of a ransomware attack is a major interruption in business operations while devices and systems are taken offline for disinfection and, hopefully, seamless restoration of clean data made possible from a well-planned backup and disaster recovery strategy. Ransomware attacks on average cause nearly 10 days of downtime.[4]

While the FBI recommends against paying ransom, it reports that more than $2.57 million in ransoms were paid in 2018.[5] On average, an organization can expect an average cost of $133,000 per attack -- all to regain access to their own data.[6] And sadly, some victims pay with no guarantee that they will recover their files and data. Studies reveal that ransomware authors generally make more than twice the average salary of developers working on legitimate projects.[7] Clearly, what works for attackers is bad for organizations and their professional IT staff.

$2.57 MILLION IN RANSOMS PAID[5]

$133,000 AVERAGE COST PER ATTACK[6]

Companies fervently hope that their anti-ransomware defenses will work. But even if they do prevent the worst—or at least partially prevent it—they may still need to contend with data loss that resulted from the attack. Average losses from an attack are about 8 percent of data.[8] In addition to attempting to get paid a ransom, attackers may extract data from a compromised computer or server, exposing sensitive data, including usernames and passwords, payment information, and email addresses of contacts. Modern ransomware attacks backup files on network shares and may even delete shadow copies on the workstation to prevent restoration. The attack and resulting data loss are a powerful one-two punch, and the risks to brand reputation can have a devastating long-term impact that severely affects credibility.

> *"Cybercriminals are becoming more sophisticated in their tactics, and seemingly no industry is immune from ransomware attacks. By targeting backup systems, hackers increase the odds that compromised organizations will make ransom payments given the severe consequences of data loss and downtime – which often extend far beyond financial repercussions. IT and business leaders must also consider the negative impact on employee productivity, customer trust, brand reputation, and regulatory compliance when systems and data are compromised."*
>
> *- Oussama El-Hilali, Arcserve Chief Technology Officer*

How are IT professionals protecting their organizations from ransomware?

A range of methods are being used to detect ransomware and protect valuable systems and data, including:

- **Ransomware protection software** to identify potential attacks, finding and preventing intrusions as they happen.
- **Firewalls** to block unauthorized access to a computer or network.
- **File filters** and **spam filterings** that block websites suspected of malware and keep unwanted attachments from entering user's email inboxes.
- **Group policy software** that blocks execution of files from local folders that can then infect the system.
- **Security Information and Event Management** (SIEM) packages that provide insight into network traffic to spot anomalies that indicate a breach.
- **Backup software** to protect business data by copying data from servers, databases, desktops, laptops, and other devices.
- **File integrity monitoring** to verify consistency between the current and a validated file.
- **Antivirus and anti-malware software** to prevent, detect, and remove malware.
- **Unified Threat Management (UTM)** solutions to address varied threats with a single point of defense and console.

While the methods to detect ransomware and protect valuable systems and data are individually important and useful, organizations are at greater risk. Today's attackers are becoming more sophisticated and resourceful. Attack strategies often combine several techniques at once, targeting separate parts of the IT network at the same time. Ransomware attacks use new malware variants to bypass antivirus programs. So, what are the pitfalls of traditional ransomware protection strategies?

Many systems lack important functionality

It was easier to tackle the malware problem when exploits could be matched with signature-based antivirus technology. As threats evolve and include distinct attacks against common vulnerabilities, it has become more difficult to identify the threats using signature-based technology.

Moreover, many data protection vendors have jumped on the ransomware bandwagon, emphasizing cyber-security "features" which, in reality, may only detect data anomalies that may or may not be ransomware related. And after detecting the anomaly, they often only provide an alert, rather than doing anything to solve the problem.

Disparate tools are hard to manage, increasing vulnerability

Many organizations use multiple tools and vendors for various security functions fighting ransomware— for example, they may use two vendors for firewalls, another for DLP or web filter, another for backup and disaster recovery, another for cloud backup, for data centers, and yet another for mobile backup.

Using separate appliances and different vendors for different security tasks makes it more difficult to track and prevent attacks. Tools and software require management and updates, making it more difficult to stay current with the latest forms of malware when several solutions are cobbled together. Managing multiple vendors and solutions increases risks, vulnerabilities and errors. Productivity suffers and costs go up.

Today, you can transform complex legacy, multi-vendor ransomware tools with a single defense-in-depth solution that features comprehensive data backup and recovery, neural network and endpoint protection against unknown malware, exploits and ransomware.

IT professionals also need IT management practices

Technology solutions are vital to cybersecurity and ransomware protection - including firewalls, intrusion detection and prevention systems and email security. Advanced solutions for integrated data security and protection go a long way toward organizational protection. At the same time, sound IT management practices are vital.

It is important to recognize that end user behaviors are the biggest threat. Organizations need to implement IT management controls that detect when employees are circumventing a policy or procedure. Management practices should include active user engagement - communicating how to adjust behaviors for security.

IT professionals must also consider their overall IT portfolio to assess risks. While any system is vulnerable to attack, the bad guys are most interested in information of value that is not adequately protected. Companies need to prioritize resource protection and use proactive IT management including Recovery Point Objectives (RPOs) to consider what amount of data loss is acceptable in the event of a failure and to shore up defenses. They need to know the resources they have and how they are configured, and they must tightly control any changes.

A framework such as Information Technology Infrastructure Library (ITIL) can help organizations execute best practices for IT management. ITIL provides practices for configuration management, change management and release management as key processes organizations can master to bolster cybersecurity and the ransomware threat.

IS BEING RANSOMWARE-FREE A REALISTIC PROSPECT?

Fending off a multifaceted ransomware attack requires a coordinated defense that combines the right technology with sound IT management practices. The ideal solution is a multi-layer, end-to-end security and protection solution. If an IT organization can deploy a first and last line of defense against ransomware, it could virtually eliminate the threat of ransomware and transform the way it protects and secures the organizations' data from extortionists, hackers, and thieves.

A recent global survey of IT professionals revealed that two out of every three respondents feel it's vitally important to find solutions that combine data security and protection.[9] These respondents deem this even more important than finding solutions that incorporate AI to predict disasters or those that automate compliance.[10]

RANSOMWARE PROTECTION STRATEGIES

Here, we outline five **ransomware protection strategies** that can help you take your organization beyond reactive security approaches and integrate anti-ransomware and other threat prevention technologies with disaster recovery and high availability capabilities to neutralize cyberattacks.

1 Actively manage access

Build the necessary controls and procedures to secure applications and systems from unauthorized users.

- Restrict access to common ransomware entry points, such as personal email accounts and social networking websites and use web filtering at the gateway and endpoint to block phishing attempts for users who are tricked into clicking on a link.
- Use multi-factor authentication and advanced password standards and include password requirements when users communicate with websites that are uncategorized by the proxy or firewall.
- Use proxy servers and ad-blocking software and restrict permissions to install and run software applications.
- Vet and monitor third parties that have remote access to the organization's network and your connections to third parties to ensure they are applying cybersecurity best practices.
- Use application whitelisting to allow only approved programs to run on a network.

2 Manage systems configuration across attack vectors

Deploy centralized management systems and procedures that address the full spectrum of ransomware threats.

- Assess and categorize business sensitive data and implement physical and logical separation of servers, networks and data stores.
- Ensure antivirus and anti-malware solutions are enabled to automatically update and scan incoming and outgoing emails to detect phishing, prevent email spoofing and filter executable files.
- Use a centralized patch management system to patch all endpoints as vulnerabilities are discovered - including on mobile devices, operating systems, software, and applications, cloud locations and IoT.
- Deploy signatureless deep learning, anti-exploit and anti-ransomware technologies that detect both known and unknown malware.
- Deploy integrated endpoint protection and business continuity technologies to accelerate threat prevention and enable immediate data restoration.
- Secure web applications and web servers using web application firewalls.
- Disable scripts from emailed Microsoft Office files and consider using Office Viewer software to open Office files.

- Audit your network for systems using Remote Desktop Protocol, closing unused ports, using two-factor authentication.
- Detect and diagnose behaviors, such as mass file encryption, as malicious and block behavior.
- Add a warning banner to emails from external sources reminding users of the dangers of clicking on links and opening attachments.
- Use Unified Threat Management (UTM) appliances that combine firewall, gateway anti-virus, and intrusion detection and prevention capabilities to block access to known malicious IP addresses.

3 Combine data security and data protection solutions

Integrate, test and maintain comprehensive cybersecurity and data protection for end-to-end protection.

- Protect backup repositories from malware, ransomware and zero-day attacks.
- Stop and remove threats such as malware and ransomware from backups.
- Keep data backups on separate devices and use offline storage where they can't be directly reached by infected devices.
- Backup virtual machines, cloud storage and operational systems based on RPOs - considering what amount of data loss is acceptable in the event of a failure.
- Use a system that allows multiple iterations of backups to be saved, in case a copy of the backups includes encrypted or infected files.
- Integrate appliances for disaster recovery and application availability and take advantage of artificial intelligence for endpoint protection.
- Use vulnerability scanning, SSL encryption, and other technical controls to confirm that backups are being performed
- Use the 3-2-1 rule by creating three copies of your data, storing them on two different media, with one of them being stored off-site.
- Routinely test backups for data integrity and to ensure it is operational.
- Routinely test data and disaster recovery processes to ensure preparedness.

4 Engage users with training and communications

Empower users with the education and practices they need to protect themselves from ransomware threats.

- Deliver regular awareness training and communications so everyone in your organization understands the threat of ransomware and is familiar with security techniques.
- Establish security and ransomware prevention policies and procedures for end users.
- Guide users to not open suspicious emails, click links or open attachments and to be cautious before visiting unknown websites and also to close their browser when not in use.
- Ensure employees know where and how to report suspicious activity.

5 Maintain and test a business continuity and disaster recovery plan

Establish, test and maintain the practices, procedures and technology tools to ensure applications and data can be fully recovered in the event of a disaster.

- Set up contingency and remediation plans which are crucial to business recovery and continuity - regardless of the source of the outage.
- Conduct a risk assessment that classifies the types of disasters that can occur and establishes priorities for recovery and business continuity.
- Deploy both onsite and offsite disaster recovery, backup, and high availability solutions.
- Have an incident response plan that includes what to do during a ransomware event, including disconnecting the infected system from the network to prevent infection propagation, determining data sensitivity.
- Test the plan – including technology systems and appliances – to ensure complete protection is delivered.
- Report any infections to appropriate authorities.

ARE YOU RANSOMWARE READY?

Download the **Ransomware Readiness Assessment** to measure your capabilities and chart a path to a ransomware-free future.

NEW TECHNOLOGY PROMISES A RANSOMWARE-FREE FUTURE

For years, IT professionals have been looking for a multi-layered, end-to-end data security/protection solution to deliver IT resiliency and ransomware prevention to no avail. The good news is now there's a solution that provides exactly that - a first and last line of defense against the ransomware threat.

This solution combines the Arcserve Appliance Series with Sophos Intercept X Advanced for Server to provide a multi-layered approach that delivers complete data protection and security—all in one unified platform.

Users benefit from the complete capabilities of self-contained systems which remove the need to source discrete components of a whole solution by delivering a central interface for backup processes, tools, and infrastructure. Arcserve Appliances uniquely deliver flash-accelerated deduplicated storage, robust server processing, and high-speed networking with highly redundant hardware and cloud services.

Add in the endpoint protection of Sophos Intercept X Advanced for Server, and you have an end-to-end solution that includes signature-based and signatureless malware detection, advanced artificial intelligence/neural network (deep learning), anti-exploit technology, and anti-ransomware technologies to deliver protection against the widest range of endpoint threats.

The result: An unmatched combination of "everything in one" – start-to-finish cybersecurity , data backup, disaster recovery, and high availability, all brought together in a single solution to fully cover every infrastructure need.

SUMMARY

While ransomware has represented a significant business risk and a menacing threat, the future is bright. Today organizations can:

- **Deploy integrated protect-in-depth solutions** for advanced backup, disaster recovery, high availability and cybersecurity;
- **Enable IT practices** with effective user engagement, data management and disaster recovery practices that realize return on investment (ROI); and,
- **Deliver a first and last line of defense** that accelerates threat detection and enables immediate restoration of backed-up data.

So why tolerate the status quo? Why put up with a world in which cyber-extortionists, hackers and thieves are using ransomware to extract ill-gotten gains from companies that are simply trying to conduct business? Fight back. Keep your data safe. Use today's end-to-end protection technology and sound IT management practices to ensure that finally, at long last, you and your organization can enjoy a ransomware-free future.

ABOUT ARCSERVE

Arcserve provides exceptional solutions to protect the priceless digital assets of organizations in need of full scale, comprehensive data protection. Established in 1983, Arcserve is the world's most experienced provider of business continuity solutions that safeguard multi-generational IT infrastructures with applications and systems in any location, on premises and in the cloud. Organizations in over 150 countries around the world rely on Arcserve's highly efficient, integrated technologies and expertise to eliminate the risk of data loss and extended downtime while reducing the cost and complexity of backing up and restoring data by up to 50 percent.

ABOUT SOPHOS

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs – a global network of threat intelligence centers.

RESOURCES

1 https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

2 https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt
https://www.aarp.org/money/scams-fraud/info-2019/survey-identity-fraud-decline.html

3 https://risksense.com/press_release/risksense-spotlight-report-exposes-top-vulnerabilities-used-in-enterprise-ransomware-attacks/

4 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

5 https://pdf.ic3.gov/2018_IC3Report.pdf

6 https://www.sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx

7 https://twitter.com/CarbonBlack_Inc/status/925348051782373382

8 https://healthitsecurity.com/news/fbi-alerts-to-rise-in-ransomware-attacks-urges-victims-not-to-pay

9 Arcserve EMEA Survey, July 31, 2019

10 Arcserve EMEA Survey, July 31, 2019

For more information on Arcserve, **please visit arcserve.com**