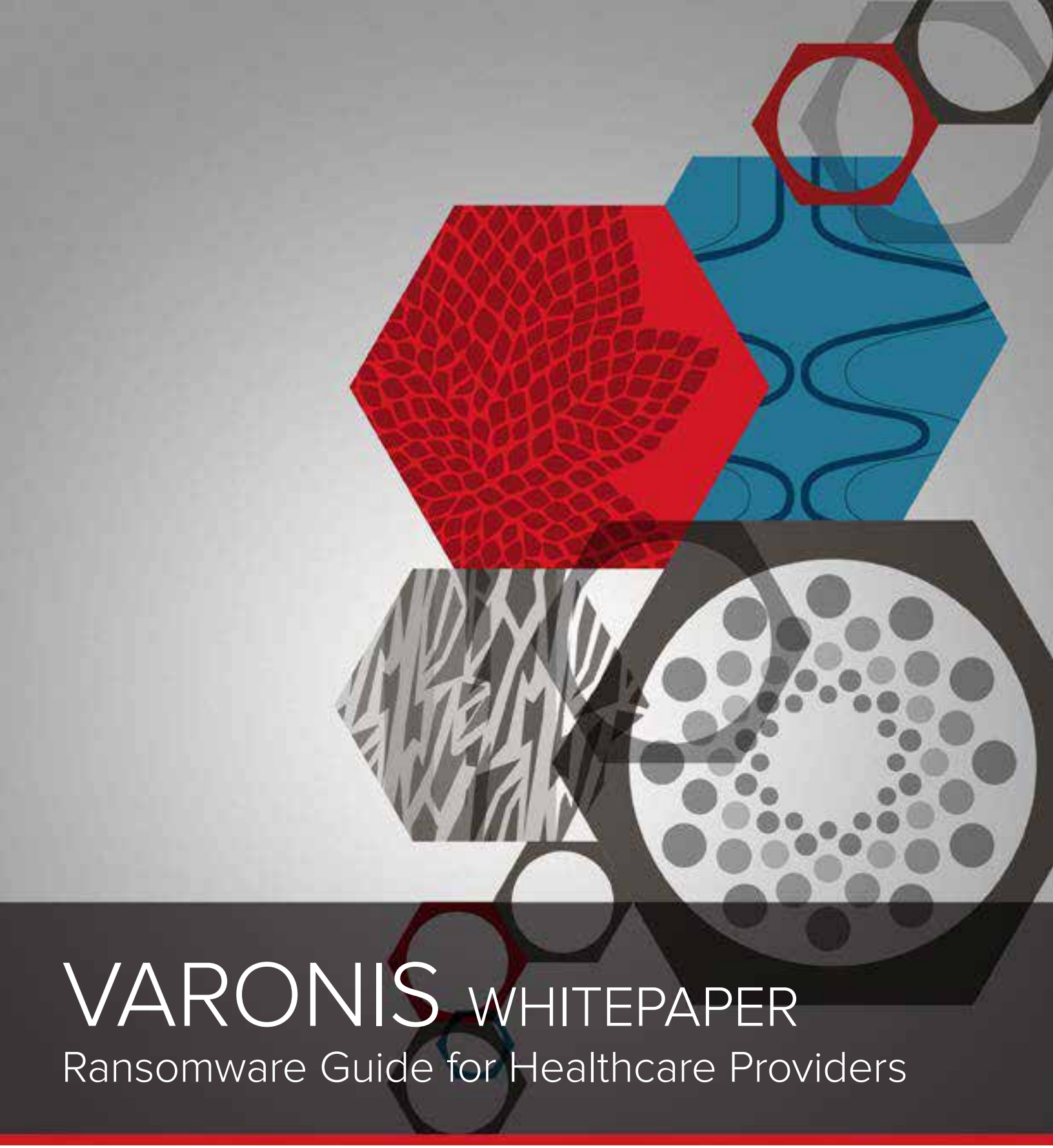

VARONIS WHITEPAPER

Ransomware Guide for Healthcare Providers

VARONIS

Towerwall

CONTENTS

THE COMPLETE RANSOMWARE GUIDE

OVERVIEW

Healthcare providers have always been attractive targets for data breaches. Why? The value of a health record is high. According to Reuters, health records are 10 to 20 times more valuable than credit card numbers. Rather than stealing health records and trying to sell them on the black market, cybercriminals are using ransomware to turn a much quicker profit.

We've seen this play out in the past couple of weeks with a rash of hospital ransomware infections. While the average ransom price is about one or two bitcoins (~$300USD), most hackers know that hospitals are willing to pay much more.

Healthcare providers depend heavily on medical systems with on-demand access to patient information. Without quick access to patient histories, medical images, and directives, patient care gets delayed, and lives are put at risk.

We've seen hospitals react to ransomware infections in different ways. Some hospitals have paid the ransom, while other hospitals restored their data from backup.

Regardless of how the hospital handled the threat, the main effect of ransomware has been downtime. It's been reported that after an infection, some hospital employees were forced for over a week to use pen and paper to enter patient data. Fax machines and phones were used to relay patient information. Patients were diverted to other hospitals. For safety reasons, high-risk surgeries were pushed to later dates.

STRAINS TARGETING HOSPITALS

As of late, according to a threat alert issued on March 30th by the U.S. Department of Homeland Security and the Canadian Cyber Incident Response Centre, Locky and Samas have been used against healthcare organizations.1

Both extremely potent, you wouldn't want either to attack. Locky encrypts data on local drives and unmapped network shares, whereas Samas encrypts your entire network.

SHOULD YOUR HOSPITAL PAY?

After a ransomware infection, your hospital is on the clock.

Against the clock, should your hospital pay? The short answer is “it depends.”

Cybercriminals are good businessmen. They’ve done the math and set a ransom so that the results will be in their favor. Their demand for a smaller hospital is a few hundred dollars, whereas a bigger hospital’s ransom is a few thousand dollars. Once the hospitals do the math, the most efficient and fastest route is to pay because lives are at stake.

One hospital that paid the ransom said, “The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key. In the best interest of restoring normal operations, we did this.”

REASONS NOT TO PAY

However, even if you pay, you might not get your files back. These are unscrupulous criminals and might have copied the health data and sold it on the dark web. Remember health records are valuable. No one says an extortionist has to honor his word.

Some hospitals that were hit with ransomware were able to restore its files from a backup and it was fairly easily since they only had one server to deal with.

But is a backup enough?

Before you decide to restore from backup, here are three things to think about:

Ransomware encrypts slowly

Ransomware variants like to slowly encrypt files before displaying a ransom note. If you're thinking about 'simply' restoring from backup, also think about how long before you would even find out your data has been encrypted?

Calculate how much downtime your hospital can handle

If you have working backups, figure out how long it would take to restore terabytes of data. You should also figure out how it impacts your agreements: Operational level agreement (OLA), Service Level Agreement (SLA), Projected Service Availability (PSA), Projected Service Outage (PSO) , etc..

Security expert Igor Bailkalov warned, "If even some of... the systems were taken down to contain the infection, full and timely restoration might be problematic."

Ransomware now deletes, destroys and/or encrypts your backups

In the past, you might be able to resort to your system backups, also known as shadow copies. Maybe if you got an infection, the ransomware wouldn't have bothered to seek out and destroy these backups. Not true, anymore.

Locky, the strain that's been targeting healthcare providers, now deletes all the shadow volume copies on the machine so that they cannot be used to restore the victim's files. Your backups will not be a deterrent. Expect your backups to be deleted or encrypted. If you want backups, it's much safer to keep recent backups off-site.

HIPAA

Would ransomware infection be considered a breach, according to HIPAA?

HIPAA is a huge law that covers the security and privacy of protect health information (PHI) held by health care providers, plans, clearinghouses, and other covered entities, as well as their business associates.

Under HIPAA, these covered entities have to report a breach to the Department of Health and Human Services—see their wall of shame—if PHI from more than 500 records has been exposed to unauthorized persons – generally speaking, hackers.

Some have said that since ransomware locks data—encrypts it and makes it unusable– and therefore doesn't expose it to unauthorized users, hospitals aren't required to report it under data breach notification rules. The HIPAA rules effectively say that if encrypted PHI is stolen or exposed, then you don't have to report a breach.

There are other opinions.

Recently, Lesley Cothran, a Public Affairs Specialist for the US Department of Health and Human Services released a statement regarding ransomware as it relates to HIPAA, "Under HIPAA, an impermissible use or disclosure of protected health information is presumed to be a breach (and therefore, notification is required) unless the entity demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment…"

What's a low probability? It's hard to say, and individual cases will vary.

Are there other potential HIPAA violations?

HIPAA's Technical Safeguards – see this primer – are one of the foundations underlying the data security regulations that companies are supposed to be following. CFR Part 164.312 section C(1) expresses the Integrity standard of PHI: its states you should have in place policies and procedures to protect electronic protected health information from improper alteration or destruction.

If you have a backup and can completely restore the locked PHI, it would appear you would not be in violation. If you don't, you might have some explaining to do to a government auditor.

And then HIPAA asks you to do risk assessments — see this Administrate Safeguards primer –and then update your controls. So even if you survived this attack, you'll need to address the issue of how the attackers got in and accessed the PHI, and then put in place procedures to either prevent or reduce the risks (see CFR 164.308(a)(1)).

Again, if you don't, you'll face the wrath of auditors and risk fines.

FURTHER READING:

- The Complete Ransomware Guide
- Why UBA Will Catch the Zero-Day Ransomware Attacks (That Endpoint Protection Can't)
- Is Ransomware the Canary in the Coal Mine?

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

ABOUT TOWERWALL

For over 20 years, the team at Towerwall has helped scores of companies safeguard their data and leverage their investment in IT with advanced information security solutions and services. As a market leader within the IT security industry, they offer complete IT security solutions and services.

Visit www.towerwall.com for more information.

Free 30-day assessment:

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

START YOUR FREE TRIAL

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.