KIRTANE & PANDIT

Ransomware: Preparing for the Imminent Threat

- Abhijit Limaye has joined us as Director -Cybersecurity Products and Services in ASG (Advisory and Solutions Group) and will be based in our Pune office.
- Abhijit brings over 27 years of industry experience with last 14+ years focused on Cybersecurity.
- He is a Master of Computer Science 1996 University Of Pune, India, First Class (68.00%) and Bachelor of Computer Science 1994 University Of Pune, India, Distinction (82.08%)
- He has held various leadership roles in companies like Symantec and Qualys leading large globally distributed product engineering and Cyber operations teams.
- At KP-ASG, he is actively engaged in building our expertise in the areas of Vulnerability Assessment (Web and IT Infrastructure), Cloud Security, DevSecOps and product-driven services.

Abhijit Limaye

B.C.S., M.C.S

Location : Pune

Practice Head : Advisory and Solutions Group

Abhijit.Limaye@kirtanepandit.com

Ransomware: Preparing for the Imminent Threat

Ransomware attacks are a growing concern for businesses and individuals alike. These attacks are designed to encrypt data and demand payment in exchange for its release. In this note, we'll explore what ransomware is, how it works, recent attacks, and more importantly what steps organizations can take to protect themselves.

What is ransomware?

Ransomware is a type of malware that encrypts the victim's data and prevents them from accessing it until a ransom is paid. The ransom is usually demanded in cryptocurrency, which makes it difficult to trace the identity of the attackers. Ransomware can be spread through infected websites, software downloads, social media messages, or phishing emails.

How does it come into user systems?

Ransomware can enter a user's system in several ways. The most common is through phishing emails, which are designed to look like legitimate messages from trusted sources. These emails often contain links or attachments that, when clicked or opened, install the ransomware on the victim's system. Ransomware can also be spread through infected websites, software downloads, or even social media messages.

Users are the weakest link in Cyber-chain

Users are often the weakest link in the security chain. Many ransomware attacks succeed because users are tricked into clicking on links or opening attachments that contain the malware. To combat this, organizations should provide regular training on how to recognize and avoid phishing emails and other suspicious messages.

Recent ransomware attacks targeting Indian Government and other organizations

Ransomware attacks are on a rise worldwide and India is not far behind.

The most recent example being the Sun Pharma ransomware attack where the company warned about direct impact to its revenues.

In March 2023, attackers targeted a Space-tech Startup which works with ISRO in a ransomware attack

In one of the biggest attacks that caused disruption for days and was widely reported, All India Institute of Medical Sciences(AIIMS) was targeted with a ransomware attack, where 5 servers and over 1.3 TB (terabytes) of data was encrypted.

Ransomware Statistics

According to CERT-In, there is a 51% rise in ransomware incidents reported until 2022-H1, compared to the year 2021 and the trend continues. No sector is spared!

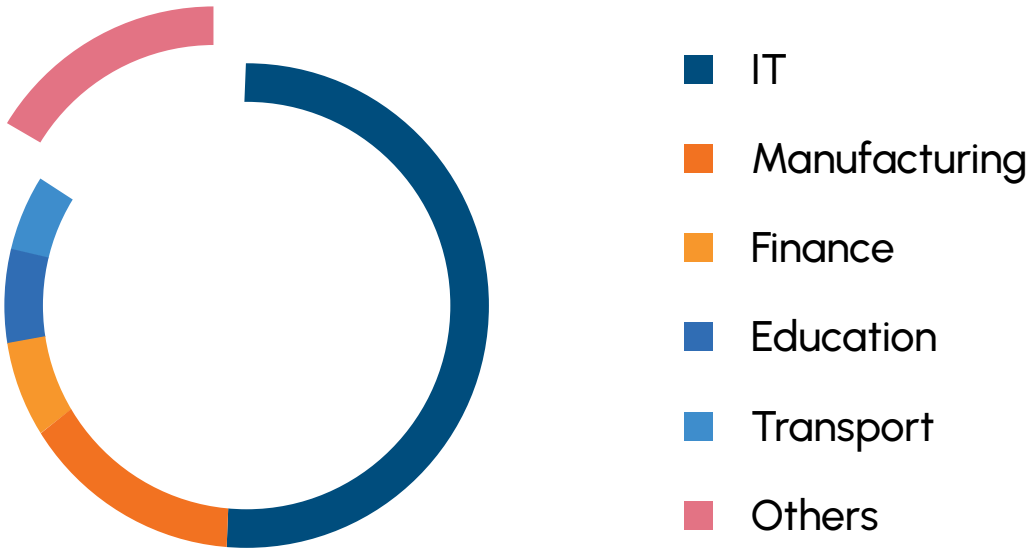
51% ▲

Overall, there is 51% increase in ransomware incidents reported in 2022-H1 compared to previous year [2021].

Major sectors affected in H1 2022

- Majority of the attacks are observed in Datacentres/IT/ITeS sector followed by Manufacturing and Finance sectors.

- Ransomware groups have also targeted critical infrastructure in H1 2022 including Oil& Gas, Transport, Power



Source: CERT-In Report: https://www.csk.gov.in/documents/RANSOMWARE_Report_Final.pdf

In recent years, there have been several high-profile ransomware attacks that have affected organizations around the world. Some of the most notable include:

- Colonial Pipeline faced a ransomware attack in May 2021. USD 4.5 million was paid in actual ransom and a 5500-mile-long gas pipeline system had to be shut down for more than 5 days. The operational impact and revenue loss could only be imagined.

- An attack on JBS - meat processing giant in the US, in June 2021, forced it to shut down all its meat processing operations temporarily resulting in operational losses. They paid USD 11 million to attackers get the decryption key for their data.

- Kaseya, an IT management software firm, was hit with a ransomware attack in July 2021. The attack had the downstream impact on over 50 Managed Service Providers (MSPs) and between 800 to 1500 companies whose infrastructure was being managed by the MSPs.. The attackers originally demanded USD 70 million in a ransom note. Kaseya did not pay the ransom but rebuilt their entire system from scratch!

▶ It is not a question of If but When!

Given the increasing prevalence and sophistication of ransomware attacks, it's no longer a question of if your organization will be targeted, but when. Therefore, it's crucial to be prepared for a potential attack.

What can organizations do?
Be prepared to defend!

▶ User cybersecurity awareness

The first line of defense against ransomware is user education. Organizations should provide regular training on how to recognize and avoid phishing emails and other suspicious messages.

▶ Patching

Keeping your system up to date with the latest Operating System and application patches ensure that systems are protected from common vulnerabilities that can be exploited by attackers to deliver ransomware to user systems.

▶ Protection

Correctly configured EPP / EDR: Endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions can help detect and block ransomware attacks. These solutions should be correctly configured and updated regularly.

▶ Data Protection, Backup and Recovery

Having a robust backup strategy with defined RTO and RPO: Backing up data regularly is another critical defense against ransomware. Organizations should have a robust backup strategy that includes frequent backups and defined recovery time objectives (RTO) and recovery point objectives (RPO).

Incident response plan

It's important to have an incident response plan in place that outlines the steps to be taken in the event of a ransomware attack. This should include steps such as disconnecting infected systems from the network, notifying law enforcement, and engaging with a cybersecurity incident response team.

Tabletop exercise

Conducting tabletop exercises can help prepare your team for a potential ransomware attack. These exercises simulate a real-world attack and allow you to test your incident response plan and identify any gaps that need to be addressed.

BC/DR exercise

Business continuity (BC) and disaster recovery (DR) exercises can also help prepare your organization for a ransomware attack. These exercises simulate impact of an attack and allow you to test your ability to recover critical systems and data.

In conclusion, ransomware attacks are a significant threat that can have devastating consequences.
By taking steps to educate users, implement a robust backup strategy, and have an incident response plan in place, you can help protect your organization from this growing threat.

We, at Advisory and Solutions Group (ASG) Kirtane & Pandit offer Ransomware Readiness as a customized service to our customers. The service offering includes all the steps described above for organization level readiness.
Get in touch with us at ASG-Cyber@Kirtanepandit.com to know more about our service offerings.

Remember, it's not a question of if, but when, so it's critical to be prepared.

Overview of Kirtane & Pandit LLP

Kirtane & Pandit LLP, Chartered Accountants (KPCA) is an Accounting, Auditing & Consulting firm with a widespread established network of financial experts across India. Our motto 'Step ahead, Always', reflects our value added approach in delivering sound financial solutions while we partner with you in your journey of growth.

With our extensive experience of 65+ years, we deliver a wide range of professional services in the areas of Assurance, Accounting & Advisory to listed & reputed companies from varied industries across the globe.

We are a registered member of PCAOB, SEC, USA & feature as an A category firm of RBI and C&AG.

- **6** decades of Experience
- Operating across India with **7** Offices
- **33** Partners
- **700+** Team of Professionals & experts
- Client spread across **30+** Industries
- Multinational Clientele parented from **17+** countries

kpca@kirtanepandit.com | www.kirtanepandit.com