CYBERSECURITY ALERT

RANSOMWARE: NEW YEAR, CONTINUING PROBLEM

ISSUED BY THE

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

OF THE

NEW YORK STATE BAR ASSOCIATION

January 21, 2021

Opinions expressed are those of the Committee preparing these Key Takeaways and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

Ronald J. Hedges
Dentons US LLP

COMMITTEE MEMBERS

Seth H. Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
Robert M. Brill
Patrick J. Burke
Ada Chan
John D. Cook
Bryan Daniels
Craig H. Effrain
Daniel H. Erskine
Hon. Fern A. Fisher
Parth N. Chowlera
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra G. Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Kenneth A. Krajewski
Anthony Lam
Christian Levis
Erica L. Ludwick
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Alexander Paykin
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Enet Somers Dehaney
Sanford Strenger
Ronald P. Younkins

CYBERSECURITY COMMITTEE MEMBERS

Seth H. Agata
Christina Ayiotis
Karim Beldjilali
Mark A. Berman
Eric Burke
Patrick J. Burke
Sasha Carbone
Nicole Cardascia
David Cass
Sarah Cole
Todd Daubert
Gail L. Gottehrer
Emma Greenwood
Ronald J. Hedges
David Horrigan
Laurie Kamaiko
Mary Kavaney
Erez Liebermann
Aishwarya Minochia
Mike Mooney
Mauricio F. Paez
Michael Pastor
Fernando Pinguelo
Debbie Reynolds
Marc Roman
Elizabeth Roper
Jay Shapiro

AUTHOR

Aishwarya Minocha

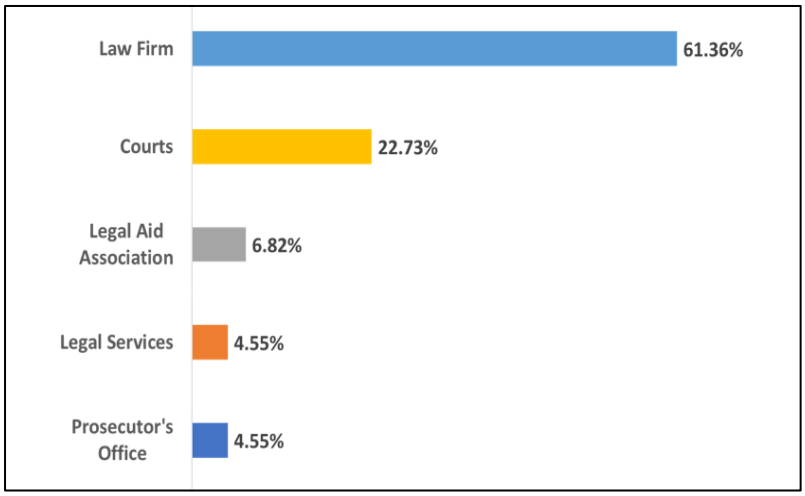
INTRODUCTION FROM THE CO-CHAIRS

Ransomware was one of the topics covered in the report about the Key Takeaways from the First Annual Cybersecurity Thought Leadership Conference that we issued in February 2020. Almost a year later, we revisit the subject of ransomware because it continues to be a significant threat to law firms, lawyers, and law departments.

We thank Aishwarya Minocha, a member of our Cybersecurity Subcommittee and a participant in both of our Cybersecurity Thought Leadership conferences, for authoring this Cybersecurity Alert. We are proud to publish her work and showcase her talent as part of our commitment to diversity and inclusion in the cybersecurity profession. Ms. Minocha co-authored our March 2020 Cybersecurity Alert on Tips for Students During the #StayAtHome Semester that provided cybersecurity guidance for students affected by the shift to online learning due to the pandemic. She has also been part of the faculty for several NYSBA cybersecurity webinars conducted by the Technology and the Legal Profession Committee.

What is Ransomware?

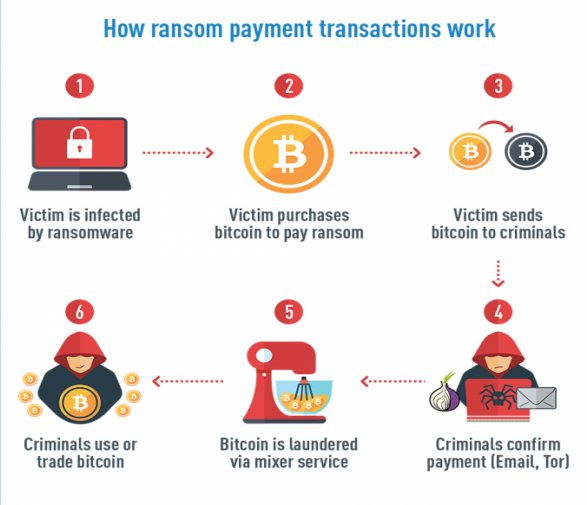
- Ransomware is a form of malicious software (malware) that targets critical data and systems for the purpose of extortion.
- Ransomware often encrypts data or programs to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data.
- In many instances, the attacker threatens to publish sensitive information that has been seized, further hurting the victim, or impacting the business' reputation.
- Ransom often needs to be paid in cryptocurrency.
- Making a ransom payment does not guarantee that the victim will regain their stolen data.



Source: T. Schreider, Ransomware Attacks in the Legal Profession, Law.com, May 26, 2020

How Ransomware Payments Work

Once the attacker has established the malware, processing the ransomware payments is the next step.



Some of the Legal Risks Associated with Ransomware

- **Confidentiality Breach**
  When attacking law firms, cyber criminals aim to obtain confidential information of the clients represented by the firm. They can use this information to demand ransom or for espionage purposes.

- **Financial and Structural Instability**
  Ransomware directed at law firms can destabilize the practices by ensuring that systems are made unavailable. Hackers penetrate systems, encrypt data, and demand high payment to decrypt it. As a result, law firms, especially the smaller ones, can be thrown into financial strain after such an attack.

- **Phony Firms Created**
  Hackers attack law firms to obtain confidential information and use it to pose as a real firm. Unsuspecting clients then share confidential information with the hackers under the impression they are sharing it with their lawyers and that the attorney-client privilege applies to their communications.

How to Respond to a Ransomware Attack

1) Isolate affected systems **immediately** - Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or shared drives. **DO NOT DELETE ANYTHING!!!**
2) Isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
3) Immediately secure backup data or systems by taking them offline - Ensure backups are free of malware.
4) Report attacks to https://www.ic3.gov/ - **Contact law enforcement immediately.** It is strongly encouraged to contact a local field office of the Federal Bureau of Investigation (FBI) or U.S. Secret Service immediately upon discovery to report a ransomware event and request assistance**.**
5) If available, collect and secure partial portions of the ransomed data that might exist.
6) If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
7) Disable maintenance tasks.
8) Implement your security incident response and business continuity plans.

10 General Preventive Best Practices

- Implement an awareness and training program.
- Use Multi-Factor Authentication (MFA).
- Use long, complex passwords and do not reuse passwords for multiple accounts. Change default passwords. Enforce account lockouts after a specified number of login attempts.
- Configure access controls—including file, directory, and network share permissions—to limit access to only those who must have it.
- Restrict user permissions to install and run software applications.
- Enable strong spam filters to prevent phishing emails from reaching the end users.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Regularly patch systems, software, and firmware.
- Configure firewalls to block access to known malicious IP addresses.
- Implement a Clean Desk Policy: https://stetsoncg.com/2020/06/19/benefits-of-following-a-clean-desk-policy/

Legal Considerations*

Enforcement by government authorities

- USA PATRIOT Act Section 314(b) encourages voluntary sharing of information among financial institutions in certain situations to identify and report suspicious activity, such as ransomware attacks.

Laws requiring breach notification

- States and regulatory agencies impose obligations on companies to provide notice of data breaches. Requirements and timeframes vary between states and regulators.

Lawsuits

- Anticipate that lawsuits, including class actions, will be filed by consumers or employees following data breaches.

*Ethical duties of lawyers regarding ransomware are beyond the scope of this Alert.