HINSHAW

Newsletters

Ransomware: The Ghoulish Battle With New Rules

October/November 2022

The Business of Ransomware – A New Normal

In the first half 2021, Accenture reported triple-digit growth in cyber intrusion activity including ransomware attacks on the world's legal, accounting, and insurance industries. In that same period, the average extortion demand rose 518 from just over $1 million in 2020 to $5.3 million while actual ransomware payments increased by 82 percent.

Ransomware payments themselves are just one category of loss caused by cyber-attacks. Others include business interruption, the costs of returning a victim's network to its original state, the legal and regulatory costs of breach notification and response, and possible litigation stemming from a breach. Together, these damages cost an estimated $20 billion worldwide in 2021.

With so much money to be made, ransomware has become big business, and the resources available to ransomware gangs now rival those of nation-state actors. For example, between April 2017 and February 2022, the Conti ransomware gang received approximately $2,707,466,220.29 in BitCoin.

Factors That Have Fueled the Ransomware Epidemic

Various factors contributed to this ransomware boom, including the rise in remote working. Hackers are also sneaking ransomware into software updates and increasing the use and sophistication of phishing and social engineering. In response to victims rebuilding networks from backups, hackers have also begun neutralizing those backups before launching an attack.

This epidemic has also been fueled by the growth of "ransomware as a service" (RaaS) where, for a monthly fee and a percentage of any extortion payment received, ransomware gangs will lease or sell sophisticated ransomware hacking tools to anyone looking for a "side hustle."

Ransomware's Impact on the Cyber Market

Cyber carriers are now actively evaluating lawyers' and law firms' cyber risk, sometimes refusing to provide coverage to those who lack sufficient safeguards. Carriers have also begun reducing their available coverage by up to 50 percent and adding exclusions to policies for known vulnerabilities.

Attorneys

Steven M. Puiszis

Service Areas

Counselors for the Profession

Lawyers for the Profession®

Litigators for the Profession®

Lawyers' Ethical Duty To Protect Against Ransomware

Model Rule 1.6 states that a lawyer "shall not reveal" *any* information "relating to the representation of a client unless the client gives informed consent, [or] the disclosure is impliedly authorized . . . to carry out the representation." This extends to disclosures "that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person."

Model Rule 1.6, therefore, obligates lawyers to take "reasonable measures" to safeguard their electronic files. This requires that lawyers take "reasonable steps" to ensure that "only authorized individuals have access to the electronic files" and that they "are secure from outside intrusion." "What constitutes reasonable efforts is not susceptible to a hard and fast rule, but is contingent upon a series of factors," including:

- sensitivity of information;
- likelihood of disclosure without safeguards;
- cost and difficulty of employing safeguards;
- the extent to which safeguards adversely affect a lawyer's ability to represent a client; and
- the client's request for or informed consent to forego certain security measures.

Other factors include the nature of a law firm's practice area(s), its size, locations, clientele, and technological sophistication. While ethics opinions explain that additional precautions should be considered in various contexts when "highly" or "particularly" sensitive information is involved, they generally do not define or discuss the types of information that would cover. Thus, law firms should address the sensitivity of client information upon retention.

Of course, the duty to take precautions does not require measures that will "guarantee" against unauthorized access. Indeed, state ethics opinions generally allow attorneys to use their "sound professional judgment" in determining what will work best. Conversely, HIPAA's Security Rule also applies to lawyers and requires various safeguards to ensure the confidentiality, integrity, and access to electronic personal health information.

An attorney's duties do not require an attorney-client relationship to exist before those duties are triggered. Rule 1.6's duty of confidentiality does not end upon the termination of the attorney-client relationship. "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client . . . shall not thereafter . . . (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client."

Given today's level of data breach risk, records and data should be kept no longer than necessary. Firms should consider developing record retention schedules and procedures to retain and securely dispose of information. At the end of any engagement, any records that can be returned to the client should be returned.

Resources:

The federal government's Cybersecurity and Infrastructure Security Agency (CISA) has a wealth of information available on ransomware defenses, including free vulnerability scanning. You can obtain this service by contacting vulnerability@cisa.dhs.gov. Once initiated, the CISA service delivers weekly reports.

Related Content

Hinshaw Insurance Law TV – Cybersecurity Third and Final Part: Ransomware

See: https://newsroom.accenture.com/news/global-cyber-intrusion-activity-more-than-doubled-in-first-half-of-2021-according-to-accentures-cyber-incident-response-update.htm [Newsroom Accenture].

https://www.paloaltonetworks.com/blog/2021/08/ransomware-crisis/

Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/#:~:text=The%20latest%20forecast%20is%20for,every%2040%20seconds%20in%202016.

KrebsonSecurity, at: https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

Model Rules of Prof'l Conduct R. 1.6(a) (2013).

Model Rules of Prof'l Conduct R. 1.6 Cmt. [4] (2013).

Ala. State Bar, Ethics Op. 2010-2 (2010).

Id. (explaining such steps include the use of firewalls, intrusion detection software and backups of all electronically stored files).

ABA Comm on Ethics & Prof'l Responsibility Formal Op. 477R (2017).

Model Rules of Prof'l Conduct R. 1.6 cmt. [18] (2013).

See, *e.g*., Ariz. State Bar, Ethics Op.90-04 (2009); N.J. Sup., Ct. Op. 701 (2006) (recognizing that a "guarantee" against unauthorized access "is impossible"); Va State Bar, Legal Ethics Op. 1872 (2013) (noting a lawyer is not obligated to "guarantee that a breach of confidentiality cannot occur when using an outside service provider").

Ariz. State Bar, Ethics Op. 05-04 (2005) ("Precisely which of these software and hardware systems should be chosen-and the extent to which they must be employed-is beyond the scope and competence of the Committee. This is the kind of thing each attorney must assess."); N. J. Sup. Ct., Op. 701 (2006) (explaining a lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access"); Mass. Bar Ass'n, Ethics Op. 12-03 (2012) ("Ultimately, the question of whether the use of Google docs, or any other Internet based data storage service provider, is compatible with [a] Lawyer's ethical obligation to protect his client's confidential information is one that Lawyer must answer for himself based on the criteria set forth in this opinion….").

See 45 C.F.R. §§160.101-160.552, 164.102-164.106, 164.302-164.318 (2014).

See Model Rules of Prof'l Conduct R. 1.18(b) (2013) (addressing information received from "prospective" clients and explaining "[e]ven when no client-lawyer relationship ensues, a lawyer … shall not use or reveal that information, except as Rule 1.9 would permit").

See Model Rules of Prof'l Conduct R. 1.6 cmt. [20] (2013); N.Y. City Bar Ass'n Formal Op. 2017-5 (2017) (noting Rule 1.6 (c)'s reasonable efforts requirement applies to "information obtained from prospective, current and former clients"). Rule 1.9(c) extends the duty of confidentiality to "former clients"). Rule 1.9(c) extends the duty of confidentiality to "former clients" and provides:

Model Rules of Prof'l Conduct R. 1.9(c) (2013).