The legal profession is not immune from the threat of a costly cyber incident. In fact, the FBI has issued warnings and held meetings with nearly all of the top law firms in New York about the risk of a data breach and theft of confidential and proprietary client information. Since at least 2009, the FBI, the U.S. Secret Service, and other law enforcement agencies have warned law firms that their computer files were targets for cyber criminals and thieves looking for valuable confidential and proprietary information, including corporate mergers, patent and trade secrets, litigation strategy, and more. In March of this year, newspapers confirmed that a Russian hacker named “Oleras” targeted 48 law firms, most of which were AmLaw 100 firms. Oleras planned to hack these firms to secure confidential and highly valuable insider information regarding mergers and acquisitions that the hacker could then use on the market.

In order to take a proactive approach to cybersecurity, it is crucial that law firms understand the type of data targeted by hackers, as well as both the legal and ethical responsibilities owed to their clients. If nothing else, from a business standpoint, many clients are now demanding that their law firms do more to protect their sensitive information to ensure they do not become ‘back doors’ for hackers. As the last installment of a four-part cyber series touching on various professional, business and insurance sectors, this article will discuss the cyber liability threat facing law firms, the ethical obligations of law firms and key security steps to implement to protect against a costly cyber incident. Additionally, in-house counsel should take a leading role in advising their client on these cybersecurity issues to help minimize the risk of litigation and fines.

ETHICAL OBLIGATIONS

Law firms have an ethical and professional duty to protect their clients’ information. Pursuant to the Rules of Professional Conduct, attorneys must take reasonable steps to protect their clients’ information. Namely, RPC 1.6(a) requires an attorney not reveal confidential information, and RPC 4.4(b) discusses an attorney’s duty to take reasonable steps in communicating with clients, as well as the duty to respect the privilege of others. Additionally, ABA Rule 1.1, Comment 8, makes clear that there is an ethical obligation related to competent representation that requires counsel to stay current on the risks posed by technology and take reasonable action to protect against those risks.

CYBERSECURITY LIABILITY

Besides the cost of remediation and reputational damage caused by a cyberattack, class action lawsuits alleging malpractice are starting to be filed against law firms for “lax” cybersecurity protections. Specifically, a complaint filed by the plaintiffs’ class action law firm Edelson PC alleges that a Chicago-based regional law firm failed to maintain robust data security practices to effectively safeguard sensitive client data. Moreover, the complaint alleges that the unidentified law firm suffered from a “number of significant data security vulnerabilities,” which resulted in “anyone with nefarious intent” – even if they were not a sophisticated hacker – likely being able to gain access to a “whole host of sensitive client data,” including the law firm’s line-item billing records and possibly email contents. Through the case, the plaintiffs’ firm and its clients are seeking injunctive relief and damages, based on the theory that the unidentified regional law firm’s clients have been overpaying for legal services because they have been paying, in part, to keep their data secure, and the law firm has failed to do so.

Aside from a claim for attorney malpractice, various state and federal regulatory agencies have taken the forefront in prosecuting claims against businesses that fail to have proper policies and procedures in place. For example, should general protected health information (PHI) be stolen, this would implicate the Health Information Technology for Economic and Clinical Health Act (HITECH). Although
sensitivity of the information, the stronger the
addition, a law firm should conduct an in-
security plan and technology.
From there, the IR Team should implement
risk assessment and remediation analysis.
Once a potential data breach has been
identified, a law firm must act quickly and
without unreasonable delay to identify the
scope and type of information exposed,
confer with internal and external experts to
ensure control and containment of the in-
cident, and preserve relevant evidence
while also preserving the attorney-client
privilege. Finally, remedial action must be
taken to correct the cause of the incident.
CYBER INCIDENTS AND THE ROLE OF
IN-HOUSE COUNSEL
A company’s board of directors has a
duty to oversee all aspects of the company’s
risk management efforts. This includes a
duty to recognize and minimize the com-
pany’s exposure to cyberattacks. In today’s
increasingly digital age, a company faces a
variety of threats to its data, including con-
fidential company information and sensitive
customer information, from rogue employ-
ees to third-party hackers. Such attacks not
only put valuable information at risk, but
can also adversely affect a company’s com-
petitive positioning, stock price, good will,
and shareholder value. Given the role the
legal department should already play in ad-
vising and directing a company’s efforts
with regard to protecting its data and re-
sponding to a cyber incident, in-house
counsel are in the best position to also help
facilitate the board’s oversight obligations.

CONCLUSION
According to most cyber experts, it is not
a matter of if, but when. These warnings
should be a wake-up call for law firm manage-
ment – and companies the world over – to
protect the enterprise’s highly confidential
crown jewels. Firms and businesses must be
prepared for a cyber incident or face not only
the costly operational, reputational, legal and
regulatory ramifications that follow but also
the loss of valuable clients. Moreover, in-
house counsel must be prepared to guide a
company in implementing a cybersecurity
program, or face potential exposure.

Other articles in this cyber series
can be found on USLAW.org:
• How to Be Secure in an Unsecure World
• Cyber Crime and The Vulnerability of the Healthcare Industry
• Will A Cyberattack On the Energy and Transportation Industries Become the Next Global Crisis?
• Keeping Customers’ Data Close to the Vest - Cybersecurity Challenges in the Retail, Restaurant and Hospitality Industry

Karen Painter Randall is a
Complex Litigation Partner
with Connell Foley LLP in
Roseland, N.J., and chair of
the firm’s Data Security
and Data Privacy and
Professional Liability Practice Groups. She pro-
vides representation and advocacy services to
professionals and businesses in a wide variety
of complex litigation matters and is a veteran
trial attorney in state and federal courts. Ms. Rand-
all, vice chair of USLAW’s Data Privacy 
& Security Practice Group and a former chair
of USLAW’s Professional Liability Group, is
designated a Certified Civil Trial Attorney by
the Supreme Court of New Jersey.

Steven A. Kroll is an
Associate with Connell Foley
LLP in Roseland, NJ. He is
a member of the firm’s Data
Security and Data Privacy
practice group. In addition
to representing professionals
in various areas, Mr. Kroll
concentrates his practice in the areas of profes-
sional liability and employment law matters in
both New Jersey and New York. Mr. Kroll re-
ceived his J.D. from Rutgers-Newark School of
Law in 2009, cum laude, and received the dis-
tinguished award of Order of the Coif.