In search of information: E-discovery and cybersecurity litigation

Prepared by:

Ryan Duquette, Partner, RSM Canada
ryan.duquette@rsmcanada.com

Sean Renshaw, National Lead, Digital Forensics & Incident Response, RSM US LLP
sean.renshaw@rsmus.com

This article was originally published by The Lawyer's Daily, part of LexisNexis Canada Inc.

In recent years, electronic discovery, or e-discovery, has grown in its application in the insurance litigation field.

While the digital landscape continues to affect businesses of all types, data collection has become more targeted across the insurance litigation spectrum. This article discusses e-discovery matters within insurance litigation, particularly within the cyber insurance industry, and highlights various benefits and challenges to this ever-growing field.

The world of e-discovery has advanced over the past two decades. What started out as scanning and coding paper documents into "electronic" documents has evolved into a vast array of tools, techniques and processes to capture, search and review electronically stored information (ESI).

Today, virtually every litigation involves some degree of e-discovery, whether it be as simple as collecting targeted emails and documents from a person, or as complex as obtaining accounting and transactional data from complex and different enterprise systems across a multinational corporation.

While the collection and review of ESI have become fairly established, there are new and innovative approaches where e-discovery is being leveraged to help reduce the cost of handling cyber events.

We have become numb to reports of cyber breaches occurring. Gone are the days when a major corporation suffered a breach and it was the leading story in every news and blog outlet. That does not mean cyber incidents have gone away; in fact, they are gaining strength and increasing with every passing day. Companies are being attacked with malware, ransomware or fall victim to a business email compromise, which frequently leads to a financial windfall for the attacker and a loss for companies and their insurance carriers.

While these are incredibly stressful and bad events, the victims and insurance companies can also face additional finance impact by having to determine if any sensitive or protected data may have been accessed, acquired or exfiltrated by the attacker (i.e., names, addresses, email addresses, login passwords, dates of birth, social security numbers and income details). So how does that tie into e-discovery? Glad you asked!

In the past, a large effort was required to identify, collect and review email and user files from systems that were compromised as part of a cyber attack. As this data was harvested, people would have to manually review it to try and parse it down to a relevant set of information that then needed to be reviewed. This smaller subset would then be used to help identify what, if any, sensitive or protected data may have been exposed.

The effort required to perform this review was very time-consuming, and in turn, costly to companies and insurance carriers. While the cost to do this for one or two compromised email accounts or laptops may be relatively minimal, imagine the cost to search an entire file server or 200 email accounts.

Companies are now taking techniques that have been refined over the past two decades as part of traditional litigations and using them to help tackle the issue of identifying and reviewing ESI to determine if it might be sensitive or protected. In general, the categories of data fall into numerous major categories such as "Communications," "Documents," "System artifacts," etc.

Traditionally, there are three phases involved in e-discovery

Phase 1: Identification, Preservation, Collection; Phase 2: Data Analysis, Reduction, Analytics; Phase 3: Processing, Review, Production

Using these traditional e-discovery processes, we can aggregate large data sets and deduplicate them, so we have a single unique population of information to review. During traditional litigation, it is important to know who had copies of what documents and emails. Responding to an incident is more about what sensitive or protected information was potentially exposed and less about who had a copy of a specific file. Once there is a unique data set, search terms can be leveraged to parse through and identify items that might contain potentially sensitive or protected information.

E-discovery searching in litigation is used to find "hot docs," privileged items, etc. Searching as part of an incident response is more binary. In essence, this means asking the question of whether this email or document contains sensitive or protected information: yes or no?

Benefits and pitfalls of e-discovery

One of the main benefits of e-discovery for cyber-insurance litigators is the ease by which large sets of data can now be parsed. In cyber incidents, all compromised data is stored digitally, so the time involved in combing through terabytes of data made the process onerous and costly. E-discovery tools continue to develop and with the advent of artificial intelligence and machine learning will likely continue to make litigators' lives easier.

Robust e-discovery also often leads to the uncovering of crucial pieces of evidence that may not otherwise have ever come to light.

Conversely, a common drawback of e-discovery can be the sheer volume of data involved. Broad requests for electronic documents can be costly and time-consuming, particularly when you consider how many electronic documents besides emails that most people come in contact with on a daily basis. Insurance litigators also often need to consider how to access and preserve evidence located in the cloud.

Improper e-discovery can lead to plenty of headaches for both sides. As more data is requested, issues such as data retention, backups and preservation processes become paramount, and sanctions and penalties sometimes result.

As litigators seek electronically stored information, working with an adviser experienced in investigating and mitigating cyber breaches can be beneficial as these professionals have a solid understanding of the cyber landscape as a whole, what type of data is attractive to attackers, how to access it and how to preserve it.

+1 800 274 3978
rsmus.com

RSM