Understanding cyberattacks and best practices in triaging breaches

A member of the nerd herd is your new best friend

Prepared by:

Sean Renshaw, Director, RSM US LLP
sean.renshaw@rsmus.com, +1 312 634 4757

July 2019

The frequency and scope of cyberattacks are growing rapidly, and breaches are a significant threat to any organization's reputation and sustainability. Media reports provide a stream of large-scale breaches on a seemingly daily basis. Interestingly, it is the smaller organizations that are at a higher risk of being breached, but less media coverage is often dedicated due to their more limited societal impact.

Regardless of the size of the cyber event, a single breach can result in significant financial, reputational and operational damage. A lesser known, but very negative, outcome of a cyber incident is the potential for government investigation or litigation. So what do you do when a cyber-related case lands on your desk or in your courtroom? How do you make any sense of all the techno-jargon that is being bandied about?

The role of forensic cybercrime experts

While not all forensic cybercrime experts are created equal, those who consult with organizations and attorneys on a regular basis are typically adept at translating "geek speak" into normal language. Highly specialized "cyber fighters" can help legal resources, risk managers, senior executives and other stakeholders navigate the often murky waters of the digital high seas. A member of this "nerd herd" can be your new best friend.

Real world example: The SamSam ransomware attack

Let's take a step back and look at what a cyber-related case may look like when it washes up on your shore.

Obviously, there have been a number of high-profile cyber incidents that have led to litigation (e.g., Anthem, Target, Equifax), but the potential for litigation is a risk for any organization. The following is a summary of a fairly complex but potentially lesser known recent case that resulted from a cyber event.

An electronic health care record provider (the cyber victim) was sued by medical institutions and health care providers as a result of a SamSam ransomware attack that it suffered, which effectively shut it down for over a week. As a result, thousands of the cyber victims' customers were unable to access patient and client information for the duration of the event.

During this time period, the victim's customers had to find alternative methods for their administration of patient health care records, resulting in a considerable disruption to health care delivery. The key facts are as follows:

- SamSam is frequently involved in cyberattacks within the health care industry and has characteristics that lead cyber investigators to believe that attacks using SamSam are often manual.
- While the cyber target hasn't publicly acknowledged the original point of compromise, a remote desktop protocol (RDP) attack is often the point of entry for a SamSam attack.
- Once the attackers have access, they are likely to use hacking tools (e.g., Mimikatz and PowerShell Empire) to survey the environment and identify potential high-value systems and IT infrastructure targets from which to launch a ransomware attack with the maximum potential business impact.

This example illustrates the challenging technical vernacular that attorneys encounter in cyber-related cases. As such, it is important for attorneys to identify a trusted advisor who can provide insight into the cyber event and be a translator and guide on this journey.

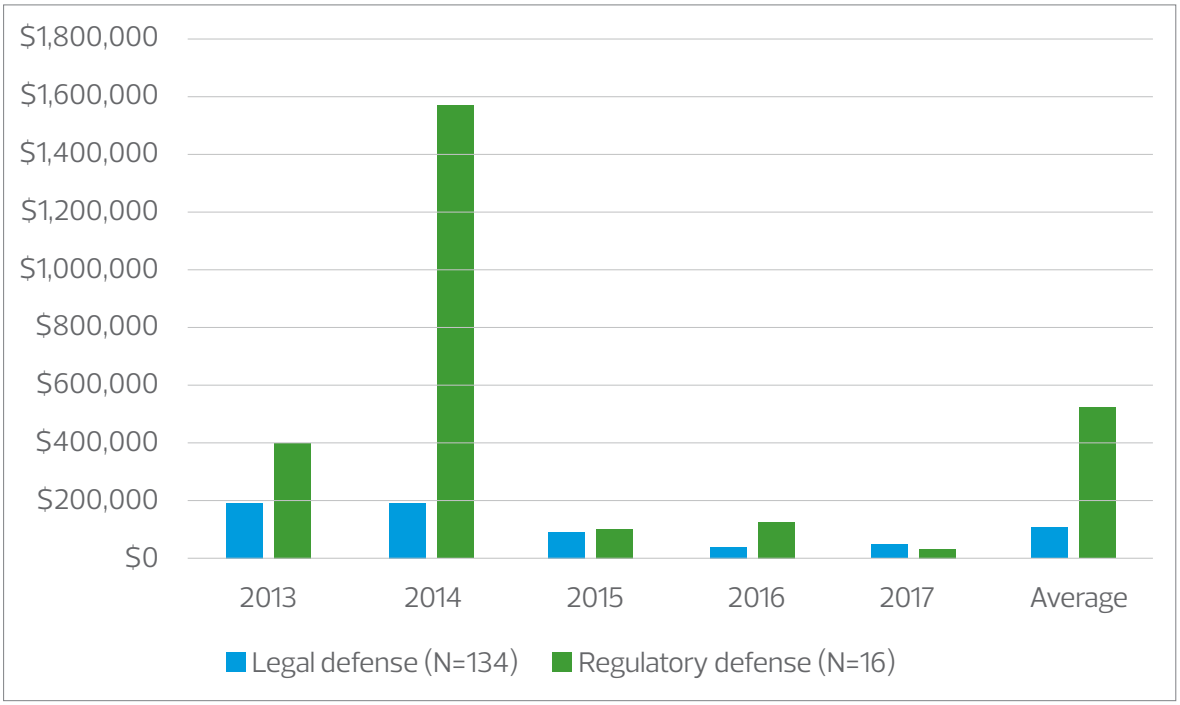
Litigation is increasing as is the cyber lexicon

The 2019 Data Breach Litigation Report published by Bryan Cave Leighton Paisner included several intriguing takeaways about the landscape of litigation relating to data breaches, such as:

- The percentage of publicly reported breaches that led to class action litigation has risen annually:
  - 2016—3.3%
  - 2017—4.0%
  - 2018—5.7%
- The complaints are mainly regarding two to four high-profile breaches
- The number of unique defendants per case is rising (26 unique defendants in 2017 and 36 unique defendants in 2018)

These facts indicate that, while the number of cyber-related litigations isn't extremely high, the number of lawsuits has been increasing along with the number of unique parties named in the lawsuits. This reflects the increased likelihood of litigation and regulatory defense costs, as noted in the 2018 Cyber Claims Study published by NetDiligence, which is summarized in Figure 1.

Figure 1—Average legal and regulatory defense costs (2013 to 2017)



So what cases are you likely to see?

While it is always difficult to predict new cyberthreat vectors, past trends are a good indicator of future cases. The following list contains a few examples of cyber issues that we believe will increasingly lead to litigation and regulatory fines:

- Business email compromises: Companies are falling victim when an attacker compromises one or more email accounts as a result of a phishing attack. The attackers can effectively take over the user's account and download all mailbox data or use their access to imitate the legitimate user and redirect financial transactions.

  Figure 2 shows the true financial impact of email account compromises, along with the resulting financial fraud, which is leading to more civil litigation between parties to try and reclaim losses. As a result, regulators are increasing pressure to investigate these types of events. In addition, more litigation is being contemplated by the parties who have lost money or did not receive payments and they are trying to recover some of the loss from another entity.

Figure 2—Business email compromise (BEC) losses

Over $12 billion in losses since 2013 due to business email compromise

Source: FBI Internet Crimes Complaint Center

Average robbery loss: $1, 373
Average BEC loss: $159,469

Sources: 2017 Uniform Crime report and FBI IC3

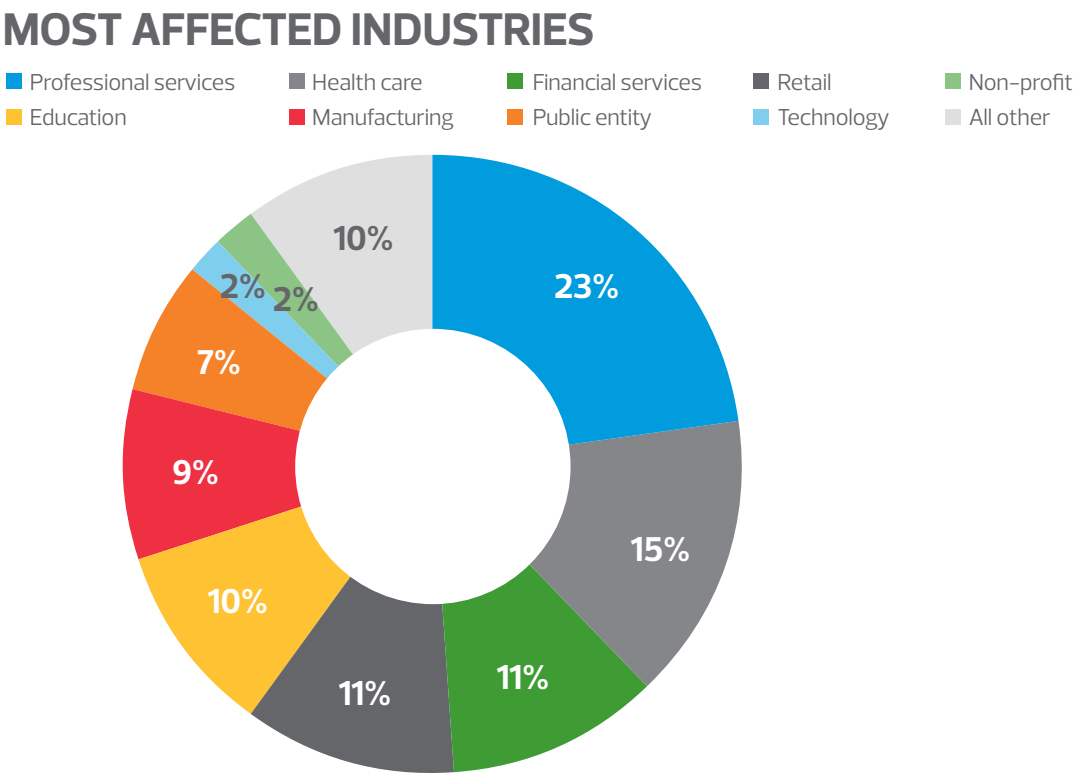
Nearly $100 million in losses for nine SEC issuers, all at least $1 million; two issuers lost over $30 million

Source: SEC Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements

- Industry is important: As noted in Figure 3, there is a significant risk to entities in the professional services (e.g., law firms and accounting firms), financial services and health care industries, which together account for nearly 50% of data breaches. These industries are especially targeted due to the type of data that can be found and stolen. For example, personally identifiable information (PII) and protected health information can be sold on the deep and dark webs and can lead to significant fraud against the aggrieved party.

  As a result, there is an increased potential for investigations or litigation surrounding these cyber incidents. Based on the statics in the Bryan Cave report, this is a consistent theme in which cyber incidents relating to PII accounted for 78% and 82% of litigations in 2017 and 2018, respectively.

Figure 3—Cyber incidents per industry (2013 to 2017)



Key points to consider

With cyberthreats evolving and becoming more prevalent, what should you do prepare yourself to handle a cyber-related matter? Attorneys will best serve their clients if they understand a number of more technical details, some of which are best rooted out by a forensic cybercrime expert (in addition to knowing leading practices in triaging a cyber-related matter). Specially trained cyber warriors—the nerd herd—help attorneys decipher key data points, such as:

1. Understanding the attack scenario:
   - What is the characteristics of the attack method (e.g., automated vs. manual, credential harvesting vs. data exfiltration)?
   - How did attacker gain access to the environment?
   - What actions did they take once inside?
2. Evaluating the entity's response to the cyber event:
   - How timely was the response?
   - Did the entity actively identify potentially compromised systems? Did the entity interrogate them to determine which actions the attacker performed?
   - Was the entity using adequate tools to identify potential attacks and malicious software?

3. Evaluating the recovery and remediation approach:
   - Did the entity have secured backup copies of key systems to get affected systems back online in a timely fashion?
   - Did the entity make sure all compromised accounts were reset and ensure that all compromised systems were remediated or rebuilt to prevent future attacks?
   - Were changes made to harden the environment and make it more difficult for another attack?

Many people with a technical IT background can answer most of these questions. However, to establish more than a timeline of the attacker's actions, effective cyber event mitigation is maximized by experienced forensic professionals who can quickly discern and communicate the relevance, importance and overall impact of an attacker's actions on the victim's systems.

Definitions used in this article:

RDP attack: RDP is a tool that is included by default in Microsoft Windows, allowing a user to remotely connect to a computer system. An attacker will find a computer in the environment that is RDP accessible and will attack the machine and take over. The attacker will then use the compromised machine to remotely connect to other systems in the environment. RDP is quite susceptible to brute force attacks in its default configuration.

Mimikatz: Mimikatz is a free tool that allows an attacker to view and steal user names and passwords. Logging into your bank account? Sure thing, it will capture that information. Checking your email? You guessed it, your credentials are compromised.

PowerShell Empire: PowerShell Empire is a tool known to be used during cyber incidents to maintain persistence within a compromised environment and allow the unauthorized user(s) to easily use other tools to perpetuate an attack.

+1 800 274 3978
rsmus.com

tl-nt-fas-bp-0719-understanding cyberattacks

RSM