DIGITAL TRANSACTIONS
Trends in the Electronic Exchange of Value

Incident-response plans should not be static. Rather, they should be living and breathing documents that are tested and updated periodically.

In Confronting Cyberattacks, Preparation Is Key

For breached retailers, responding after the fact is responding too late, say Aaron P. Simpson and Chris Hydak.

Aaron P. Simpson (top) is a partner at Hunton & Williams LLP, where Chris Hydak is an associate.

It's clear that cybercriminals have zeroed in on the retail industry, primarily on account of the sheer volume of payment card information available, combined with the perception that state-of-the-art safeguards—or even adequate information security, in some cases—are lacking.

Cybercrime in the retail environment is a highly scalable enterprise, allowing successful criminals to siphon mountains of payment card information that can be monetized quickly on the black market. This scalability is evident in the jaw-dropping numbers revealed by Target and The Home Depot after their recent cyberattacks, which saw each company report that tens of millions of consumers were impacted.

Not only do these cyberattacks result in significant expense, they also trigger a complex array of legal considerations, including exposure to significant liability. Managing cybersecurity risk in this environment has proven to be a daunting exercise. But, through careful planning, retailers can go a long way toward successfully mitigating their cybersecurity risk.

Massive Compliance Effort

As a technical matter, malware was the big story in the retail industry in 2014. The Secret Service estimated that over 1,000 U.S. businesses were impacted by the Backoff malware. Backoff is particularly ominous, given its ability to scrape payment card information from the point of sale, where the information is unencrypted in memory for a fleeting moment post-swipe.

The costs borne by retailers victimized by Backoff and other cyber threats have skyrocketed. A survey by the Ponemon Institute found that the average annual cost of cybercrime to U.S. retailers in 2014 was $8.6 million. This was more than double the average annual cost in 2013. Given the number of retailers thought to be impacted by Backoff alone, the financial impact to the industry is staggering.

Unfortunately for retailers, the parade of horribles resulting from a cyberattack does not stop at technical remediation. It also includes a bevy of legal considerations and potential liability.

Depending on the circumstances, liability can be significant and include reimbursing issuing banks for costs associated with fraudulent charges and reissuing payment cards, as well as paying fines assessed by the card brands to merchant banks that are passed down to breached retailers by contract.

In addition to this potential liability, retailers suffering a cyberattack must comply with a patchwork quilt of data-breach notification laws in 47 states, Washington D.C., Puerto Rico, Guam, and the U.S. Virgin Islands. After a breach is announced, it has become relatively commonplace to receive inquiries from state attorneys general and/or the Federal Trade Commission, as well as complaints from lawyers

representing consumers and business partners alleging significant damages.

Making matters considerably more complex is that each jurisdiction's breach-notification law applies to its residents, regardless of the location of the purchase. Thus, retailers with a significant geographic footprint, both online and off, typically face a massive compliance effort in navigating the legal landscape in the aftermath of a breach. And they must do so under a tight timeline while simultaneously restoring the integrity of their systems.

The Time Is Now

Fortunately, there may be relief in sight. Although the concept of a national breach-notification standard has been discussed for years in Congress, President Obama proposed the Personal Data Notification & Protection Act on Jan. 13.

While the upside of this proposed legislation is that it contains a national breach-notification standard that preempts state law, the downside is that the obligations it imposes are uniformly onerous, including:

- A presumption that notification after 30 days following the discovery of a data breach is "unreasonable." The Ponemon Institute found that the average time to resolve a cyberattack for U.S. companies in 2014 was 45 days. Insider attacks take even longer to resolve.
- A significant expansion of the definition of personal information, including data elements that could trigger even more notification obligations for retailers. Such databases might contain marketing lists or loyalty-program information, for example.
- A requirement to notify affected individuals unless "there is no reasonable risk of harm or fraud" to the affected individuals. This high threshold, combined with the need to conduct a risk assessment and report the results to the FTC in order to rely on it, creates a more onerous standard than the majority of existing state laws with respect to consumer harm.

Given that the likelihood of a cyberattack has moved from an "if" question to a "when" question, the key to managing risk is appropriate planning. From a legal perspective, a nonexistent or ill-conceived incident-response plan represents a significant gap and is all too common among retailers.

Cyberattacks are interdisciplinary events for impacted retailers. They often involve representatives from information services, legal, communications, marketing, privacy, and human resources, as well as outside advisors and other third parties. Getting this diverse group of professionals rowing in the same direction on the fly under an intense time crunch when facing an actual breach is simply impossible. The time is now for retailers to develop a plan if they do not already have one.

Mitigating Legal Risk

A well-conceived plan requires many components to be successful. Chief among those components are effective identification of potential breaches, seamless escalation/triage, and clearly defined roles for those involved in the containment and remediation process.

Once developed, incident-response plans should not be static. Rather, they should be living and breathing documents that are tested and updated periodically.

While there is no single step retailers can take to ward off cyberattacks, a thoughtful incident-response plan will facilitate smoother breach remediation which, in turn, serves to mitigate legal risk after the breach is announced. DT