THE ANATOMY OF A

CYBER INCIDENT RESPONSE

Best Practices for Insurance Claims Professionals Handling Data Breach Losses

By Stuart A. Panensky and Anthony J. Dolce

Companies dedicate significant resources to avoiding data breaches and managing other cyber risks. As a result, cybersecurity is a growing field within larger corporate IT, and has caught the eye of senior management. In fact, many companies' C-suites now either include a chief information security officer (CISO) or have a CISO reporting to them.

However, when failures in cybersecurity occur for small and mid-size enterprises, an appropriate cyber insurance policy can be an invaluable tool to assist businesses with responding to, and dealing with, the aftermath of an incident. A cyber insurance policy provides a risk-transfer mechanism, and offers some protection from the vast menu of cyber and data-security risks.

Following a cybersecurity event, it is the claims professional who assists the policyholder in navigating the sometimes complex and often stressful ordeal, and it is the claims professional who truly has a 360-degree view of the entire process. Let's discuss the lifecycle of a cyber insurance claim and examine basic best practices for the insurance claims professionals who handle these matters.

DISCOVERY OF THE INCIDENT

The first milestone in the lifecycle of a cyber claim begins when the policyholder discovers that a cyber or privacy incident has occurred. There are multiple ways that cyber incidents are discovered by policyholders. Many IT-related security breaches are discovered by the company's internal or outsourced IT teams. The teams either detect unusual activity or receive a report from a user. Sound corporate incident-response policies dictate that the IT professional should advise someone in management about the incident, who would then determine if notifying the cyber insurer is appropriate.

In some cases, law enforcement agents advise companies during a criminal or national security investigation that they have experienced a cyber incident. For policyholders in the retail industry, notification may also stem from law enforcement's work with the payment card industry (PCI) in credit card fraud investigations. Additionally, card brands and law enforcement investigate common points of purchase amongst stolen credit card credentials and will alert merchants if there is evidence that one of its PCI systems was compromised.

ROLE OF CYBER BREACH COUNSEL

Once an incident is discovered and reported to a cyber insurer, the response process begins. At the outset, the best practice is for the cyber claims professional to ensure that the policyholder retains qualified cyber breach counsel to coordinate the response efforts.

The prompt retention of counsel is important to maximize the availability of the attorney-client privilege—in order to facilitate the response efforts, the attorney must be in a position to offer privileged counsel to the policyholder. It is common to learn unflattering things about a policyholder's IT network or corporate privacy practices during the response process, so the proper establishment of the attorney-client privilege can help facilitate these difficult conversations.

Accordingly, it is important for the attorney-client relationship to be formed between the cyber breach counsel and the policyholder as early as possible. It is equally as important for the claims professional to respect, and help maintain, the attorney-client privilege between the policyholder and retained counsel. In this scenario, counsel, rather than the policyholder, would retain third-party vendors to assist in the investigation of the claim.

The first consultant that the breach counsel retains is typically an IT forensics consultant to conduct an independent, third-party analysis of the incident. The issues that the IT forensic investigator examines include, but are not limited to, the fundamental cause, origin, and scope of the incident. The investigator will also make recommendations for remediation.

The most significant issue for cyber breach counsel is determining whether there was any data exfiltration or wrongful disclosure of sensitive data, including personally identifiable information, protected health information, financial information, or other sensitive data.

Claims professionals must be cautious and understand that not all data that is wrongfully disclosed is sensitive data that triggers legal obligations. A certain amount of analysis and investigation must be overseen by cyber breach counsel to offer appropriate recommendations to the policyholder to ensure that the policyholder is aware of, and is addressing, its legal obligations.

IT IS COMMON TO LEARN UNFLATTERING THINGS ABOUT A POLICYHOLDER'S IT NETWORK OR CORPORATE PRIVACY PRACTICES DURING THE RESPONSE PROCESS, AND THE PROPER ESTABLISHMENT OF THE ATTORNEY-CLIENT PRIVILEGE CAN HELP FACILITATE THESE DIFFICULT CONVERSATIONS.

NOTIFICATION

To the extent forensics determines that there was exfiltration of sensitive data, breach counsel must analyze the policyholder's legal obligations to notify

the impacted individuals, the government, credit ratings agencies, and/or the media. In doing so, breach counsel must identify and analyze the applicable legal authority and counsel the policyholder regarding its notification obligations.

All U.S. states have some version of a data breach notification law. Many industries that are regulated by the federal government, like health care and financial services, may have additional data breach notification requirements mandated by federal law. Policyholders that do business with residents of the European Union may also have notification obligations under the General Data Protection Regulation's (GDPR) data breach notification requirements.

Several states permit substitute notification of a data breach to be made via the media (as opposed to individually notifying every person) in situations where the data breach has impacted a large number of that state's residents. This substitute notification is separate and apart from the potential media inquiries that a business may face as a result of a data breach. Thus, it is generally advisable that a business be prepared to respond to such inquiries by retaining a public relations firm to coordinate external communications.

REGULATORY REPORTING AND INVESTIGATION

In addition to notifying impacted individuals, many state data breach laws require policyholders to notify a government agency of the incident. For example, most state laws require companies to notify that state's attorney general about the incident.

While there is no universal federal data breach notification statute, certain federal laws also require notification to a government agency if sensitive information was compromised. For example, under federal HIPAA laws, health care companies are required to notify the U.S. Department of Health and Human Services' Office of Civil Rights.

After notification, these government agencies will often initiate civil investigations of the incident itself and the policyholder more generally. The breach counsel works with the policyholder to respond to the government and reach a resolution to the investigation. Sometimes, this resolution results in fines and penalties or an order from the government instructing the policyholder to do something—or not do something—relating to cybersecurity and privacy.

PAYMENT CARD INDUSTRY

For incidents involving retail merchants, claims professionals may have to deal with losses stemming from a PCI investigation, which is very similar to the government investigations described previously. However, this investigation is presided over by a group of representatives from the payment card industry and involves a separate forensic investigation of the policyholder by a PCI-authorized quality security assessor who reports directly to the PCI.

This security assessor has no obligation to the policyholder. Breach counsel will work with the policyholder (and often a payment card processor) to advocate during the PCI investigation process, which often also results in a separate set of fines, penalties, and assessments.

THIRD-PARTY LITIGATION

Finally, after all of the above has been performed, the first third-party claim will be made either by one of the individuals notified about the incident, or by another impacted organization alleging damages were suffered and proximately caused by the incident. Given that most cyber insurance policies contain both first- and third-party insuring agreements, it is at this time when the cyber claims professional returns to his traditional third-party claims-handling role.

These third-party lawsuits allege many different theories of liability, including negligence, breach of contract, or a violation of a statute, and often require attorneys with specific skill sets to appropriately defend. The claims professional must evaluate these liability issues early on in order to make appropriate decisions for the balance of the claims-handling process.

OTHER BEST PRACTICES

It is important to note that cyber insurance policies vary from carrier to carrier, and with manuscript policies, can even differ among two different policyholders that have the same carrier. The policyholder should always refer back to its specific policy to determine what is covered.

In the case of ransomware occurrences, data exfiltration is not always an issue, so there may not be any legal obligations on the part of the policyholder. The claims professional's objective in these cases is to handle the matter like an emergent first-party claim, bringing to bear the appropriate resources to assist with expeditiously getting the policyholder's data back to its original pre-attack condition (if possible). For the same attorney/client privilege-related reasons outlined earlier, use of breach counsel for ransomware occurrences is still the best practice.

A cyber claims professional should also be cognizant of the potential interaction with other insurance policies that a policyholder may have, and how such coverages may impact the claim at hand.

As cyberthreats continue to evolve and become more damaging, policyholders expect cyber insurers to have sophisticated claims operations that follow best practices when handling cyber claims. Accordingly, cyber insurance should be considered a key piece of a policyholder's incident response plan, and the expertise of the cyber claims professional is an important resource that should not be overlooked. ■

Stuart A. Panensky is a partner at FisherBroyles, LLP and a leader in its cyber risk, privacy, and data security practice group.
stuart.panensky@fisherbroyles.com

Anthony J. Dolce is vice president and claims cyber lead for North American financial lines claims at Chubb.
adolce@chubb.com