COVINGTON

Manage Ransomware Risks Now

May 17, 2017
Insurance

Last Friday may mark the start of a new era in cyber crime. The first worldwide ransomware attack, commonly dubbed "WannaCry," emerged on May 12. The malware is believed to have infected more than 300,000 computers in 150 countries to date. A cyber criminal or ring of criminals, taking advantage of an exploit made available by the ShadowBrokers hacker group that reportedly uses tools stolen from the U.S. National Security Agency, propagated an attack that installs malware to encrypt users' data unless a ransom in Bitcoin is paid within a few days. While the actual ransom payment losses have reportedly been minimal, the more serious result of these attacks has been the disruption to victims' business activities.

The attacks highlight the need for risk management focused on ransomware attacks. This includes not only cybersecurity prevention measures and advance preparation of well-defined cyber incident response plans, but also the careful review of insurance protection. This alert provides practical guidance from Covington's insurance recovery team on some of the insurance issues that ransomware attacks pose for businesses.

Insurance Coverage for Ransomware Attacks

Even if your organization was unaffected by this latest ransomware attack, other bad actors will likely be inspired to follow suit. Before the next attack occurs, organizations should review their insurance policies to determine what coverage they may have in the event of a ransomware attack, and then take steps to plug any gaps they may find. The potential losses from a ransomware attack may implicate various types of insurance, including cyber, property, general liability, and kidnap and ransom (K&R) policies. Some issues to look out for in that review include the following:

- The "cyber extortion" coverage option offered in cyber policies, and sometimes in K&R policies, is the logical first place to look for protection against the more immediate impact of ransomware attacks. This coverage typically reimburses costs to investigate an extortionist's threat to attack the insured's computer system and (with insurer approval) to pay off the extortionist.
- In recent years, some cyber insurers have added specialized ransomware endorsements that require closer attention. Among other things, they may operate as functional exclusions masquerading as coverage grants, by imposing extremely small sublimits on the otherwise available cyber extortion coverage (which may itself be sublimited).
- Both cyber extortion and ransomware coverage wordings require close reading, particularly in their definitions of the covered risk. For example, by focusing too narrowly on past vectors of attack, they may fail to encompass the latest mutation in attack methodology, such as the self-propagating WannaCry worm.
- The most significant financial losses to a business whose computer system has been attacked are likely to be for forensic investigation costs and business interruption. Policyholders need to ensure in advance that their policies cover those losses effectively

in a ransomware situation. For example, while most cyber extortion insurance forms cover forensic work relating to the extortion attempt, many require advance insurer approval; and some cover only the immediate costs to prevent or terminate the extortion threat, while others extend to root cause investigations. Cyber-related business interruption is a coverage option under many cyber policies and some K&R policies, and it is now offered as a coverage extension by major property insurers. If this coverage is found in multiple lines of insurance, then careful comparison of deductibles and waiting periods, as well as "other insurance" clauses, is necessary to determine which applies first. In addition, the wordings of these non-standardized coverage grants require special attention to ensure that they encompass all potential ransomware attack vectors and all the critical systems likely to be interrupted by such an attack.

- As for the ransom itself, the insurance review should confirm the availability of coverage for Bitcoin, the currency of choice for cyber criminals. Older policy wordings may not unambiguously encompass Blockchain technology or unofficial, virtual currencies.
- Beware of exclusions affecting your particular business. For example, cyber policies routinely exclude bodily injury, a ransomware-related risk that a health care provider could plausibly face. General liability or errors and omissions policies traditionally cover bodily injury, but now may contain cyber-related exclusions. Specialty policies or specifically negotiated endorsements may be needed to fill this gap.
- Finally, look for both policy conditions and policy application questionnaires that relate to the insured's network security practices, and try to qualify them appropriately. For example, a representation in the application that the policyholder keeps all software up-to-date may provide fodder for a coverage defense if the policyholder (like many victims of the WannaCry worm) delayed patching a software vulnerability. This is especially problematic if the policy wording itself purports to give the insurer the right to deny coverage for errors in maintaining network security. (In UK policies, for example, insurers are increasingly characterizing the insured's compliance with specified obligations as conditions precedent to their liability to pay claims).

If you have any questions about the issues discussed here, or need help with your insurance strategy, please contact the following members of our Insurance Practice Group:

John Buchanan	+1 202 662 5366	jbuchanan@cov.com
René Siemens	+1 424 332 4751	rsiemens@cov.com
Richard Mattick	+44 20 7067 2023	rmattick@cov.com
Scott Levitt	+1 202 662 5661	slevitt@cov.com

If you have questions about, or require assistance with, ransomware incident response planning, please contact the following members our Cybersecurity Practice Group:

David Fagan	+1 202 662 5291	dfagan@cov.com
Jenny Martin	+1 650 632 4737	jmartin@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.