Consider Ransomware Now So You Don't WannaCry Later

Last Friday, a massive wide-scale cyberattack involving a ransomware software program called Wanna Decryptor, also known as "WannaCry," swept the globe, freezing computer systems and causing major disruptions. The attack — which is the largest ransomware infestation ever — affected tens of thousands of organizations across the globe and a wide range of industry sectors, including the United Kingdom's National Health Service (NHS), Spanish telecom giant Telefonica, France's car-maker Renault, Portugal's Telecom, and the United States delivery company FedEx, among many others. As of Monday, the attack reportedly has affected nearly one hundred and fifty countries.

Ransomware (a combination of the terms malware and ransom) has become an increasingly common form of cyber extortion. It often involves extortionists taking control over a computer system and locking files and data on the system by encryption, thereby rendering them inaccessible, and useless, until a demand for payment, typically in Bitcoin, is satisfied. A typical form of ransomware, WannaCry does the following: 1. locks all data on the victims' computer systems, 2. informs victims that their files have been encrypted, 3. warns that those files will be deleted unless payment in Bitcoin is received, and 4. provides instructions for executing and sending the payment.

Ransomware has become frighteningly pervasive and increasingly serious and expensive. Ransomware attacks quadrupled from 2015 through 2016, to an estimated 4,000 per day according to the United States Department of Justice and, as punctuated by WannaCry, are projected to double yet again in 2017. These types of cyberattacks can, and do, cause significant operational disruption, often halting a business in its tracks, reputational damage and other types of losses and exposures. Every industry sector is seeing an increasing threat, with the healthcare and education sectors particularly targeted. Other forms of cyberextortion, including threats to obtain or release protected information, such as personally identifiable customer data, protected health information and confidential corporate information, or to discharge denial-of-service attacks that disrupt an organization's networks, causing business interruption, also entail significant potential exposure to organizations.

Here we offer five insurance and other considerations for organizations to consider in the face of an enormous uptick in increasingly severe ransomware attacks and other forms of cyberextortion:

1. Consider purchasing "cyberextortion" insurance. No firewall is unbreachable, and no security system impenetrable. In the context of this reality, insurance can play a vital role in a company's overall strategy to address, mitigate, and maximize protection against the legal and other exposures flowing from serious cybersecurity, privacy and data protection-related incidents. Importantly, almost all stand-alone so-called "cyber" insurance policies offer

coverage for ransomware and other forms of cyberextortion. This type of coverage is specifically designed to cover losses and expenses that an organization incurs in the wake of a cyberextortion incident like the WannaCry software virus, together with myriad other forms of first and third-party cybersecurity and data privacy-related exposures, including coverage for crisis management (such as notification to potentially impacted individuals, credit monitoring, and call center services), data breach and network security-related claims and liability, including regulatory liability, business income loss, and digital asset loss. Cyberextortion coverage can be extremely valuable as a way for organizations to address and mitigate losses arising from mounting extortion threats, and many organizations now purchase this coverage as part of their cyberinsurance programs.

2. Closely review cyberextortion insurance terms and conditions. It is clear that cyberinsurance can be extremely valuable, but obtaining the right insurance product presents significant challenges. There is a diverse and growing array of cyberinsurance products in the marketplace, each with its own insurer-drafted terms and conditions that vary dramatically from insurer to insurer — and even between cyberinsurance policies underwritten by the same insurer. In addition, the specific needs of different industry sectors, and different organizations within those sectors, are far-reaching and diverse. For these reasons, organizations purchasing cyberinsurance, and the cyberextortion components of that insurance, are well advised to closely review the terms and conditions of the coverage to ensure that the organization's cyber extortion risk will be covered, without a protracted battle with the insurer, in the wake of an attack. Among other things, organizations are advised to consider the following:

    - Scope of coverage. Cyberextortion coverage should written to cover as broad a range of potential attacks, and potential exposure outcomes, as possible. The coverage should include any threat to negatively impact, impair access to or engage in unauthorized access to, relevant computer systems and the applications, files and data residing on those systems, together with any threat to access or divulge any sensitive information in the organization's possession or control.

    - Key definitions. Key definitions must be sufficiently broad to match the reality of risk faced by the insured organization. By way of example, in addition to definitions that define the scope of coverage, definitions governing the types of losses and expenses that are covered should be carefully reviewed. The policy should cover reasonable and necessary expenses incurred by the insured organization resulting from a covered threat, including the costs of investigating and assessing a threat (even if no ransom is paid), should expressly cover payment of cryptocurrencies (including Bitcoin), as well as, preferably, any other consideration or action that may be demanded by the extortionists, and should cover reasonable and necessary expenses incurred to mitigate or reduce other covered expenses.

    - Conditions. Organizations are advised to pay close attention to policy conditions, including notice and consent provisions, proof of loss provisions, allocation provisions, alternative dispute resolution provisions and any requirements that the organization notify law enforcement of the incident at issue. The importance of

notice provisions is addressed in further detail below. Consent provisions may be favorably amended to state that an insurer's consent to satisfying the extortion demand "shall not be unreasonably withheld". Other provisions, such as the requirement of involving authorities, may be deleted. As discussed more below, cyberinsurance policies are highly negotiable and very favorable amendments can often be made for no additional premium charge.

- Exclusions. It also is critical that organizations be aware of any insurance policy exclusions that may vitiate the coverage that the policy was intended to cover. By way of example, cyberinsurance policies typically contain a "bodily injury" exclusion. Such an exclusion may pose a particularly problem for hospitals and other health care providers, which rely on access to patients' medical records to provide appropriate care and treatment. As with other exclusions, it may be possible to significantly curtail or delete bodily injury exclusions. Many other types of exclusions can be curtailed or deleted — often for no additional policy premium.

- Sublimits and retentions. It is clearly important that a cyberinsurance sublimit of liability (a ceiling on the amount of coverage available to cover a specific type of loss at issue) be sufficient to cover the organization's potential exposure. Like other facets of cyberinsurance coverage, including coverage for losses associated with regulatory action and PCI DSS-related liabilities, cyberextortion coverage may be written subject to a relatively low sublimit, such that, for example, a $10 million limit primary policy may provide only $250,000 or $500,000 for cyberextortion losses. In addition to policy limits, organizations are advised to pay attention to self-insurance features, such as policy retentions or deductibles, which typically range from $0 to excess of $5 million. As with the case of other cyberinsurance terms and conditions, sublimits and retentions usually are negotiable. On a related point, as discussed further below, what starts with an extortion threat can end up triggering many different modular aspects of cyberinsurance coverage. It therefore is important that the policy contain a provision stating that an extortion threat, together with any other first or third-party covered events that trigger different coverage sections of a policy, are subject only to a single retention, and that any lower retention amount applicable to a particular coverage section, such as a cyber extortion section, is met when that lower retention amount is satisfied by payment of loss under that coverage section.

  Although placing coverage in this dynamic space presents a challenge, it also presents substantial opportunity. The cyberinsurance market is competitive, and cyberinsurance policies are highly negotiable. This means that the terms of the insurers' off-the-shelf policy forms often can be significantly enhanced and customized to respond to the insured's particular circumstances. Frequently, very significant enhancements can be achieved for no increase in premium. Before an attack occurs, organizations are encouraged to proactively negotiate and place the best possible coverage in order to decrease the likelihood of a coverage denial and litigation. A well-drafted policy will reduce the likelihood that an insurer will be able to successfully avoid or limit insurance coverage in the event of a claim.

3. Provide notice and comply with other policy conditions. Insurance policies typically contain notification provisions stating that the insured organization must provide notice within a certain time frame, often "as soon as practicable," even "immediately," after the organization becomes aware of an incident. Although providing notice to an insurer may not be top of mind in a cyberattack situation, particularly where the demand is far below the policy retention or deductible, it is important for an organization to reasonably comply notice provisions (and other policy conditions, including consent provisions) in order not jeopardize, or delay, coverage. In the context of providing notice, moreover, it is important for organizations to recognize that what begins as a relatively low cyberextortion demand may quickly evolve into an incident or series of related events that triggers other first-party coverage sections of the insurance policy, such as the business income loss coverage (an extortion event may result in a significant loss of business income), extra expense coverage, digital asset loss recover/restoration coverage and crisis management coverage and, to the extent personally identifiable information or protected health information may have been compromised, for example, the third-party claim coverage sections of the policy, including coverage for data breach-related lawsuits and regulatory liability. Indeed, a ransom demand may be deployed as a purposeful diversion from a different, principal goal, such as stealing sensitive records. Recognizing this reality, it is important that the organization be aware of, and reasonably comply with, notice provisions in order to avoid a coverage defense based on purported late notice. In addition, providing notification can provide the insured organization with valuable coverage for costs related to the extortion threat, such as a forensics investigation, which may reveal other malware on the computer system, stop the intrusion, and block future extortion attempts, a consultant to utilize decryption keys or to recreate the files and data at issue, and, where appropriate, legal counsel. The bottom line: in the event of a cyberextortion demand, organizations are advised to provide notice under all potentially implicated policies, excepting in particular circumstances that may justify refraining to do so, and to carefully evaluate all potentially applicable coverages.

4. Maximize coverage across the entire insurance program. Although cyberextortion coverage is an obvious place to look for coverage in the wake of a ransomware attack or other cyberextortion incident, organizations are advised to consider all potentially applicable insurance policies and coverages. As noted above, a cyberextortion incident may trigger various other coverages under the organization's cyberinsurance program, and also may trigger other insurance policies and programs, such as computer crime policies and kidnap and ransom policies. The various types of insurance policies that may be triggered by a cyberattack likely carry different insurance limits, deductibles, retentions and other self-insurance features, together with various different and potentially conflicting provisions addressing, for example, other insurance, erosion of self-insurance and stacking of limits. For this reason, in addition to considering the scope of substantive coverage under an insured's different policies, it is important to carefully consider the best strategy for pursuing coverage in a manner that will most effectively and efficiently maximize the potentially available coverage across the insured's entire insurance portfolio. Absent a compelling reason, notice should be provided under all policies that potentially provide coverage.

5. Exercise business continuity and improve computer security. Insurance aside, the best protection against a ransomware attack is to have all files and data securely backed up, in a

separate physical location, or at least on a separate system, so that no business-critical information that is not recoverable may be permanently deleted by extortionists. It also is important to reflect on how these types of attacks occur. Cyberextortionists must download malicious software onto a system, or a connected device, and this often is achieved through tricking employees to click on attachments or links in phishing emails, which increasingly look convincing. Therefore, improving computer security, including through antivirus programs, spam filters, firewalls, installation of software updates and security patches (early reports indicate that WannaCry appears to exploit a vulnerability in Windows that Microsoft patched on March 14, which would have automatically protected those computers with Windows Update enabled), disabling of macro scripts, and utilizing application whitelists, which only allow approved files to execute, is essential. Likewise, training employees about how to recognize and avoid social engineering exploits such as phishing emails, is key in negating or minimizing ransomware threats. Organizations also are advised to consider incorporating ransomware attack scenarios into their incident response planning.

A well-negotiated insurance program, together with solid business continuity planning and comprehensive, proactive cybersecurity policies and procedures, will position an organization to be resilient in the face of the serious and escalating threat posed by cyberextortion. For more information, please contact Roberta D. Anderson at (412) 297-4970 or randerson@cohenlaw.com. To receive future news alerts, please send an e-mail to bulletins@cohenlaw.com.

This article first appeared in the May 15 edition of the Law360. Law360, Los Angeles (May 15, 2017, 10:55 PM EDT)