advisory

WHY CYBER INSURANCE IS NOT ENOUGH

In case the title of this article creates any ambiguity, let that be resolved right away: cyber insurance is a good idea. Cyber breaches are an undeniable part of 21st century reality, and any business thinking that a robust Privacy and Security program will automatically shield it from a sanctionable event is engaging in a legal strategy known since Roman times as *pium desiderium*. Wishful thinking.

While there are often situations where any strategy is better than no strategy at all, when it comes to equipping your organization to deal with today's cyber threats, a strategy of wishful thinking is the equivalent of no strategy at all. In the increasingly likely event that you find yourself preparing to brief the board on your organization's response to an investigation by the HHS Office of Civil Rights, or FINRA, or the *Wall Street Journal*, expect to hear the question "Are we insured for this?" Perhaps unsurprisingly, any answer other than "But, of course" may have an immediate impact on one's job security algorithm. While cyber insurance is a good idea, anyone relying on a cyber insurance policy – standing alone – to protect an organization from harm badly misunderstands the nature of cyber insurance and the protection it provides.

What Cyber Insurance Is and Is Not (and Why)

To understand why a cyber insurance policy is not enough, it helps to understand what cyber insurance is and what it isn't. A cyber insurance policy is not an off-the-shelf, one-size-fits-all coverage agreement like the insurance that gets foisted upon you every time you rent a car. Cyber policies offer a wide range of "insuring modules," covering a variety of potential risks. An applicant can select only those risks that apply to that organization and can hedge its bets as to some or all the risks that do apply. Cyber insurance has historically not been cheap, and it only gets more expensive as deductibles go down and the scope and limits of coverage go up. Cyber insurance applications have historically taken a lot of time and effort and require serious decisions to be made.

What cyber insurance also is not is a strategy. It is not a front-line defense to privacy and security risks. So, as an aside, when the conversation turns to compliance with the European Union's General Data Protection Regulation (GDPR), a description of your organization's response that leads with the phrase "We've added it to our cyber insurance policy" is probably not a good sign.

Another thing cyber insurance is not is predisposed toward payment. This much should be clear: insurance is like a trip to Vegas, where the carrier is the house and you are the player. Some players walk away with the house's money; but, in the aggregate, the house always wins. It must. Thus, the more often the house can avoid payout, the more often it will. Cyber insurance is no different. Cyber insurance is not a replacement for the policies, procedures and training that, if properly implemented, may reduce your organization's legal exposure should it ever be effectively targeted. Better yet, those policies, procedures and training may well reduce the likelihood that your organization will ever actually need to invoke coverage under your cyber policy.

Focus on the Fine Print of Cyber Policies

An interesting trend seems to be materializing in the realm of cyber insurance application forms: they are sometimes getting shorter. Anyone who obtained a cyber insurance policy five years ago will recall what a detail-intensive application it required. Today's applications are frequently much shorter and less intensive. Rather than documenting the details of the organization's privacy and security policies, an applicant today is more likely to be asked merely to certify that the organization is in compliance with the applicable laws and regulations underlying the coverage modules sought.

Anyone who thinks that this trend is the result of some focused marketing effort by carriers to become more customer-friendly should think again. The primary effect of the trend toward certification-based application formats is to give carriers a basis on which to deny coverage and, if possible, even to deny the duty to defend. If an administrative body concludes that a security incident demonstrates that your organization is or was out of compliance with some provision of HIPAA, PCI, GDPR, some obscure NIST protocol, or whatever might apply to the insuring modules you have selected, that administrative finding may demonstrate that your organization has breached its certification that it was, and shall remain, in compliance with all applicable law. If you read your policy, it will effectively communicate that a breach on your behalf frees the carrier from its obligations under the agreement.

The Courts Weigh In

To reinforce the statements above that cyber insurance is a prudent if not downright necessary part of any 21st century Enterprise Risk Management strategy, one need merely look to a recent case decided by the United States District Court for the Southern District of Florida. *See Brush v. Miami Beach Healthcare Grp. Ltd.,* 238 F. Supp. 3d 1359 (S.D. Fla. 2017). In *Brush*, a group of healthcare providers was sued by its patients after an employee of the group sold those patients' personal data. Of more than passing note, the court denied the patients' Breach of Contract action, which rested upon the fact that the breach constituted a violation of the group's Notice of Privacy Practices. That Notice of Privacy Practices, without more, did not imbue the group with a contractual obligation. However, the court refused to dismiss the patients' Negligence claim, noting: "It is well-established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information." *See id.* at 1365 (citing Liam M. D. Bailey, *Mitigating Moral Hazard in Cyber-Risk Insurance,* 3 J.L. & Cyber Warfare, 1, 11 (2014) (financial institutions and healthcare providers possess a very high duty to protect consumer data residing on their networks); *Resnick v. AvMed, Inc.,* 693 F.3d 1317 (11th Cir. 2012) (finding implicitly that healthcare providers owe patients a duty to protect sensitive data); *Weigberg v. Advanced Data Processing, Inc.,* 147 F. Supp. 3d 1359, 1363 (S.D. Fla. 2015) (finding that ambulance provider had duty to exercise reasonable care in safeguarding and protecting sensitive information)).

Along with the trend toward certification-based application forms, the odds of an insured finding itself with no coverage seems more likely following recent court decisions that focused on disparities between the terms of coverage and the specific causes of action pled by the victims of an insured's breach. For example, the United States District Court for the District of Utah recently denied a motion for summary judgment brought by cyber policy holders who sought a determination that the carrier owed them a duty to defend. *See Travelers Prop. Cas. Co of Am. v. Fed. Recovery Servs.,* 103 F. Supp. 3d 1297 (D. Ut. 2015). The related-company policy-holders provided processing, storage, transmission, and other handling of electronic data for customers. They were sued for conversion, tortious interference, and breach of contract by a health club client after they transferred the client's reports to a successor in files that allegedly did not contain critical information like its members' credit card and bank account information, and allegedly demanded additional compensation. When their cyber insurance carrier denied even a duty to defend, the insureds sued the carrier and sought summary judgment.

In denying the insureds' motion for summary judgment, the court held that the allegations in the health club's complaint did not constitute the "errors, omissions and negligent acts" covered by the cyber policy, such that the carrier had no duty to defend. It would be reasonable to expect the average executive executing a cyber policy to have anticipated at least a duty to defend in that fact pattern. The incomplete transmissions that undoubtedly represented a breach of contract could have been the result of an honest "error, omission or negligent act," which the policy covered. Denying the insured's arguments that the duty to defend should remain until any uncertainty as to coverage was resolved, the court specifically stated that there was no ambiguity when none of the underlying actions sounded in negligence.

A similar focus on the nature of the underlying claim is found in a case involving a cyber policy holder labelled by the carrier as a high risk, "PCI Level 1" client because it conducted more than 6 million electronic payment transactions per year. *See P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No. CV-15-01322-PHX-SMM, 2016 U.S. Dist. Lexis 70749 (D. Ar. May 31, 2016). PCI DSS, or the Payment Card Industry Data Security Standard, is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. After the insured's credit card servicer assessed fees related to a certain "account data compromise event," the insured attempted to invoke its coverage. The insured even identified which clauses of the cyber policy it believed to cover the specific fees issued.

In upholding the denial of coverage (and in dismissing the complaint against the carrier, to boot), the court noted that the policy covered injuries resulting from actual or potential unauthorized access to private personal information. Since the credit card servicer had not had its private personal information breached, the court held that it had no standing to bring the type of privacy-related claim covered by the policy. Thus, the Privacy Notification Expense fees levied by the insured's credit card servicer were not covered by the insured's cyber policy. It's a fair bet that this insured never anticipated that outcome when it signed up for a policy marketed as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world" that "[c]overs direct loss, legal liability, and consequential loss resulting from cyber security breaches." *See id.* at *2.

Be advised, therefore, that some federal courts have held that cyber insurance policies only cover causes of action specifically listed in those policies. If you have a cyber insurance policy, break it out and identify how much of the coverage is written in discrete causes of action. You may discover that the policy you bought is not sufficient to protect against the scope and breadth of cyber risks your organization actually faces.

To return to whence we began, cyber insurance is a good idea. However, it is not a substitute for a robust compliance program, it may not cover anywhere near the range of contingencies the policy holder thinks it does, and it may require certifications that jeopardize the very coverage being sought. Compounding this, courts seem to be taking a much more cause-of-action based approach toward interpretation than is likely contemplated by the organizations shelling out for coverage.

So, what is the lesson to be learned here? It can, perhaps, be best summed up by yet another maxim that's been around since Roman times. *Caveat emptor.* That one likely needs no translation.

Joel K. Goloskie

Senior Counsel

Joel K. Goloskie is Senior Counsel with Pannone Lopes Devereaux & O'Gara LLC and a member of the Health Care, Litigation, Cyber Law and Corporate & Business Teams. His experience ranges from compliance and HIPAA privacy matters to regulatory filings and approvals, contract drafting and management, and mergers and acquisitions. He has assisted health care clients as they dealt with compliance orders and deferred prosecution agreements, and has represented clients in both civil and criminal matters in federal court.

PANNONE LOPES DEVEREAUX & O'GARA LLC

counselors at law

This memorandum is intended to provide general information of potential interest to clients and others. It does not constitute legal advice. The receipt of this memorandum by any party who is not a current client of Pannone Lopes Devereaux & O'Gara LLC does not create an attorney-client relationship between the recipient and the firm. Under certain circumstances, this memorandum may constitute advertising under the Rules of the Massachusetts Supreme Judicial Court and the bar associations of other states. To insure compliance with IRS Regulations, we hereby inform you that any U.S. tax advice contained in this communication is not intended or written to be used and cannot be used for the purpose of avoiding penalties under the Internal Revenue Code or promoting, marketing or recommending to another party any transaction or matter addressed in this communication.