May 2-3, 2021

CYBERHEADACHE RELIEF: Actionable Intelligence for Counseling Union Clients

Marc S. Mayerson[1]
The Mayerson Firm PLLC
www.mayersonfirm.com
Washington, DC

Organizations are dependent upon their communications and computer systems, and such systems serve as vectors for adverse events that can cause loss to the organization. Consequently, insurance instruments are available to help mitigate the risk and facilitate the recovery from computer-related losses.

Confronting the cyber-insurance market is bewildering. According to one study, in 2019 there were some 580 different insurance companies selling cyber

[1] Marc Mayerson is a lawyer, arbitrator, mediator, expert witness, and law professor. He represents policyholders in insurance-recovery matters and counsels clients on property-casualty and related insurance coverage. During his three decades plus career, he has recovered millions of dollars from insurers in favor of unions and pension plans. In addition to co-editing the leading insurance practice guide (*New Appleman*, Lexis), Marc writes and lectures extensively on insurance issues, including on cyber-insurance issues, see *Insurance Recovery for Year 2000 Losses* (Andrews June 1998); *Insurance Coverage for E-Commerce* (Coverage Sept 2001); and *Insuring Against Cybercrime* (The Recorder Feb. 3, 2012). Marc also provided expert testimony on ERISA bonding requirements to the 2018 Advisory Council on Employee Welfare and Pension Benefit Plans (the ERISA Advisory Council to the Secretary of Labor). Marc can be reached at marc@mayersonfirm.com or 202.517.6607.

insurance.[2] In many sectors of insurance, there is standardization of policy wordings; this is not the case in cyberinsurance. Scores of different cyber-insurance policy forms are in use, but some uniformity of terminology has been achieved as a consequence of the heft of the top ten writers of cyber coverage, which together command more than 60 percent of the market.[3]

Organizations of all types and sizes are incurring cyber-related losses.[4] And the size of loss is not necessarily correlated with the size of the organization. According to a recent study, for firms with fewer than 9 employees, reported cyber losses ranged from $8000 to $300,000+.[5] US-based organizations have seen increases in "ransomware" attacks with more than 70 percent of targets paying ransom.[6] In a typical ransomware attack, the victim incurs additional costs, effectively doubling the total loss, in recovering its operations.[7]

---

[2] Federal Insurance Office, US Department of Treasury, *Annual Report on the Insurance Industry,* p. 68 (Sept. 2020).

[3] According to the Federal Insurance Office report (p. 69), the top ten in order of premiums collected were:

Chubb Ltd
American Insurance Group
AXA SA
Travelers Companies, Inc.
Beazley PLC
Axis Capital Holdings
CNA Financial Corp.
Liberty Mutual Holding Co.
BCS Insurance Co.
Fairfax Financial Holdings Ltd.

One study reviews more than 100 cyber insurance policy forms, Romanosky et all, *Content Analysis of Cyber Insurance Policies: How do carriers write policies and price cyber risk?* available at https://www.ftc.gov/system/files/documents/public_comments/2017/10/00012-141437.pdf

[4] One summary is Verizon's annual Data Breach Incident Report, available at https://enterprise.verizon.com/resources/reports/dbir/

[5] *Hiscox Cyber Readiness Report 2021* at p. 9.

[6] *Id.* at 10.

[7] *Id.* at 11.

Courts and regulators require entities and their leaders to protect the organization from cyber-losses.[8] Recently, for example, the Department of Labor's Employee Benefits Security Administration on April 14, 2021, issued three cybersecurity guides: "Tips for Hiring a Service Provider[9]," "Cybersecurity Program Best Practices[10]," and "Online Security Tips.[11]" Today, a robust computer-security program will include the purchase of cyberinsurance.

Most cyberinsurance offerings include both risk transfer to the insurer and free and discounted services through preferred providers. The differing policy wordings and different service offerings makes comparing cyber-insurance policies extraordinarily difficult from the buyer's perspective.[12] Differentiating what might be covered under a cyberinsurance policy and what might *already* be covered by existing policies is labyrinthine at best, and insurers (AIG and Lloyd's, as examples) increasingly are trying to preclude such "silent cyber" coverage expressly.[13] Although following a major loss it behooves the insured to explore

---

[8] *E.g., In Re Caremark Int'l Derivative Litigation*, 698 A.2d 958 (Del. Chg. 1996).

[9] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/tips-for-hiring-a-service-provider-with-strong-security-practices.pdf

[10] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf

[11] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf EBSA's action follows a GAO report concerning cybersecurity risks in retirement plans. *See* GAO, *Defined Contribution Plans: Federal Guidance Could Help Mitigate Cybersecurity Risks in 401(k) and Other Retirement Plans* (Feb. 2021) (GAO-21-25 available at https://www.gao.gov/assets/gao-21-25.pdf). *See also* Advisory Council on Employee Welfare and Pension Benefit Plans, Cybersecurity Considerations for Benefit Plans (Nov. 2016), available at https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/about-us/erisa-advisory-council/2016-cybersecurity-considerations-for-benefit-plans.pdf

[12] Thus, working with a competent insurance intermediary is key, though such intermediaries (brokers and agents) owe little to no duty of care in presenting options for the insured. *See, e.g., Merrick v. Fischer, Rounds & Associates, Inc.*, 305 Neb. 230, 939 N.W.2d 795 (2020).

[13] That such "silent" or unexpressed coverage exists was the premise of the article I co-wrote twenty years ago concerning insurance recovery for ecommerce losses. *See* Mayerson (with Johnston), *Insurance Coverage for E-Commerce: What Companies Need to Know*, 11 Coverage at 20 (Sept/Oct 2001) (available at https://www.mayersonfirm.com/articles-and-publications). No doubt cyber-insurers are more ready to make payments for cyber-losses than is true for insurers with "silent" cyber coverage. For example, the Indiana Supreme Court recently ruled in favor of coverage regarding whether a Crime policy covered a ransomware attack. *See G&G Oil Co. of Indiana, Inc. v. Continental Western Insurance Co.*, No. 20S-PL-617 (Ind. March 18, 2021). The unfortunate insured in *G&G Oil* filed its suit in mid-2018, and

recovery under any available insurance,[14] the focus of in-house lawyers and outside counsel providing advice to clients today should be on key elements of dedicated cyber-insurance products.

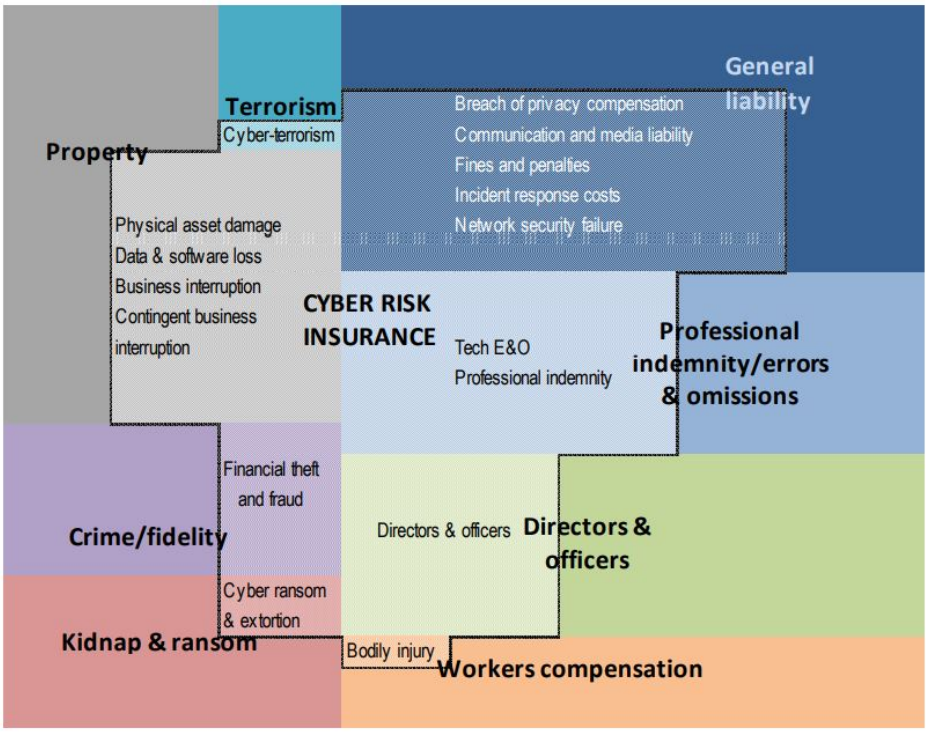
Most cyber-insurance policies bundle together several coverages. Many of these are of little value to labor unions and affiliated organizations, but are included in the standard offering of the nearly 600 insurance companies in this market.[15]

---

following its successful appeal on the point of law still needs to try the case three years' later against the insurance company on remand.

[14] The chart below shows how specialized cyber-insurance policies might overlap with the broad array of policies typically purchased:

Figure 4.1. **The potential for overlapping coverage for cyber risk in stand-alone and traditional policies**



Source: OECD based on JLT Re (2017).

OECD (2017), *Enhancing the Role of Insurance in Cyber Risk Management*, available at http://dx.doi.org/10.1787/9789264282148-en; *see also* OECD (2020*), Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation*, available at www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

[15] As one academic study observes:

Absent some unique exposures, for the most part unions do not need to focus (much) on the following coverages in a proposed cyber policy:

Business Interruption/Dependent Business Interruption
Media Liability
Cyber Terrorism
Employee Privacy/HIPAA
Payment Card Liability, PCI Fines and Costs

For unions, the focus should be on these three:

Data breach implicating personal information that requires notification
Social Engineering/Fraudulent Funds Transfer
Ransomware.

And some policies limit or exclude coverage in the event that proper internal computer security protocols are not followed; one should search for such trapdoors, too.

1. Data Breach and Notification Coverage

For many organizations and business, data about customers are key assets or are subject to special privacy-protecting regulations (HIPAA for example). Unlike intellectual-property assets held by pharmaceutical or technology companies, unions do not possess "digital crown jewels" that incentivize cyber-intrusions.[16] Nevertheless, unions and affiliates routinely maintain records about their members,

> There also are dozens of different cyber policy forms being sold that are so dense that one needs to retain experts in both cyber security and insurance to even attempt to make an educated purchase. The cyber policies currently being sold also provide inadequate actual insurance coverage because the coverage grants are narrowly written and then subject to a prolix of exclusions.

Christopher French, *Five Approaches to Insuring Cyber Risks*, 81 Md. L. Rev. at 29 (Forthcoming 2021).

[16] Put differently, information maintained by unions is unlikely to be perceived to be of value to the criminal market, and unions therefore are more likely to suffer a breach from a broader, undifferentiated hacking attack that searches widely for an open door to the network or via a low-level phishing effort.

some of which may be subject to newer privacy regulation.[17] Such stray personally identifiable information if exposed to hackers may trigger statutory notification requirements.

In reviewing a proposed insurance policy, notification-cost coverage typically can be found in a specific insuring agreement providing "cyber incident response" coverage, "breach response costs," or "security event costs." Those terms will be defined in the policy to include expenses of notifying individuals whose personally identifiable information or protected information may have been impacted.

Along with coverage for notification and other compliance costs, such insurance will cover various expenses for forensic analysis and reconstruction.

2. Ransomware

Organizations of all sizes have been victimized by ransomware. In a ransomware attack, users are locked out of all or part of the organization's computer system.[18] According to a recent survey, in more than two-thirds of cases, the victim pays ransom; sometimes they pay ransom more than once.[19] Sophisticated ransomware attacks include partial disclosures by the perpetrators of damaging information and contacting customers directly to taunt the victim. Unions are not likely targets of such attacks, but the increasing profitability of this criminal enterprise and the increasing availability of ransomware-as-service and of hacking tool sets underscores that any organization can fall victim to a ransomware attack. The most likely vector is a phishing email that installs malware on the network but various network exploits also have been used.

Coverage for ransomware-related loss will be found in an insuring agreement for "cyber extortion" or "network extortion" or other wording referring to "threats" and extortion.

---

[17] As a matter of cyber-housekeeping, it may be worthwhile to evaluate what data has previously been collected and whether any fields (containing protected information) can be purged (deleted) without impairing unduly the organization's objective in collecting that information in the first place.

[18] Sullivan and Muir, *Ransomware: A Perfect Storm* (RUSI for Defense and Security Studies (2021), available at https://rusi.org/publication/emerging-insights/ransomware-perfect-storm

[19] *Hiscox Cyber Readiness Report 2021.*

Perhaps the greatest value in ransomware insurance is simply having a process in place and people to call. Ransomware events are traumatizing for organizations, and a key benefit of high-quality insurance is the associated peace of mind the insurer provides through ransom negotiators, confirmation of proof of life (*i.e.*, ability to restore the network if ransom paid), and facilitation of payment through crypto-currency. (Insurers also are keenly aware of the need to comply with OFAC and FinCen requirements re funding of terrorism and crime.)

3. Social Engineering

One common form of cyber-related loss is based on fraudulently impersonating a valid payee of an organization and through that ruse obtaining funds. The paradigm is that an authorized user transfers funds. (A hacker has not broken in and hijacked the computer system directly, which may be covered as an "unauthorized use" or "computer fraud" coverage.) A specific insuring agreement (or separate endorsement) applies for "cyber crime," or "eCrime," or "social engineering."

The coverage will indemnify the insured for direct financial losses as a result of a fraudulent instruction, funds transfer fraud, telephone fraud, or social-engineering fraud.

4. Key Exclusions

Mapping what a particular cyber-policy covers to the insured's range of risk is taxing at best and migrainous at worst. Though many of the exclusions appearing in cyberpolicies appear (more or less) sensible in context, one aspect of some cyber policies merits special attention; in general, although policyholders think that accidental losses are covered by their insurance, this may not be so under some cyber policies.

Drawing on supposedly analogous concepts such as requiring sprinkler systems as a condition of fire insurance, in cyber policies the insured typically makes a continuing promise to employ hygienic cyber practices. Under some policies, however, if the insured negligently fails to patch its systems and a loss occurs, the insurer might deny coverage completely. An example of such an exclusion is the following:

> "Failure to ensure that the computer system is reasonably protected by security practices and systems maintenance procedures that are equal to or superior to those disclosed in the [policy application]."

In a different insurer's policy, the same type of limitation occurs regarding social-engineering coverage, as follows:

> "[Covered] Fraudulent Instruction will **not** include loss arising out of [such] instructions received by the Insured *which are not first authenticated* via a method other than the original means of request to verify the authenticity or validity of the request."

This is not to gainsay the importance of instituting robust internal procedures on computer security and funds transfers. Although the insurer's desire to incentivize reasonable conduct is understandable, these negligence-limitations are still traps because they arise at the point of claim. (Union procedures likewise instruct persons not to be negligent while driving, though undoubtedly everyone expects coverage to apply even when an individual does not meet that standard.) If the insurer is not satisfied with the computer-security practices of an insured, it should not sell it the policy, or not renew, or even cancel prospectively; the vice is that these exclusions spring after the policy incepts and when loss occurs.

5. Fortifying the Insurance and Cybersecurity Relationship

Regardless of one's experience with insurers in other lines of business, insureds should consider their cyber-risk insurers as part of their own IT/InfoSec/Privacy team. Over the next decade, cyber-insurance might evolve to be comprehensive outsourced IT management, with all cyber-risk-transfer built in. Meanwhile, leading insurance companies include both risk-transfer and a menu of services for free or at a discount.

Once insurance is in place, the insured absolutely should use the insurer's preferred providers and take advantage of the discounted good-housekeeping services the insurer-vetted vendors provide.

For example, one insurer offers a network-security and procedures audit for a flat-fee of $3000 from a leading provider. (In this regard, EBSA's recently released Cybersecurity Program Best Practices calls for a "Prudent Annual Risk Assessment," which the insurer's offering might well satisfy.) Similarly, training programs for employees on cyber-security and anti-phishing are available for free or at discounted rates. Free or discounted password-software and multi-factor authentication methods for network access typically are available via the insurance company.

The cyberinsurance underwriting process itself will prompt the insured to confirm their updates of security procedures and practices, which facilitates putting such matters on the organization's agenda.[20] A vigorous effort to respond to an underwriting questionnaire ensures that internal stakeholders commit to cybersecurity every bit as much as they commit to HVAC and other critical operating costs.

More important, at the time of loss, insurers have an entire infrastructure in place to assist the insured in crisis. Insurers often have designated "breach coaches," which are lawyers with specialization in privacy or ransom as the case may be. Because the insured only will need a breach coach during crisis, it is advisable to review in advance the insurer's proposed list and identify a suitable candidate (that is, one without conflicts of interest against the union, for example). The leadership team literally should have the breach coach and insurer's breach hotline on speed dial, because when the phone number is needed the computer system may be inaccessible!

(Please note that a call to the breach coach in an emergency generally is not the same as providing notice to the insurance company, which should be promptly effected via the separate track specified in the policy.[21])

---

[20] *See generally* J. R. C. Nurse, L. Axon, A. Erola, I. Agrafiotis, M. Goldsmith and S. Creese, *The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes*, 2020 INTERNATIONAL CONFERENCE ON CYBER SITUATIONAL AWARENESS, DATA ANALYTICS AND ASSESSMENT (CYBERSA), 2020, pp. 1-8, doi: 10.1109/CyberSA49311.2020.9139703.

[21] *See generally* Marc Mayerson, *Perfecting and Pursuing Liability Coverage: A Primer for Policyholders on Complying with Notice Obligations*, 32 Tort & Ins. L. J. 1003 (1997).

The insurance company also will have several preferred computer-forensic providers, whose services will be available at a discount or whose costs might be fully reimbursed by the insurance company. If the insured wishes to use a different vendor, the insured either might forfeit coverage or receive only a reduced payment for the services provided.

The bundle of services provided can be thought of as a "put option" in the event of a cyber crisis. Absent a compelling reason, the prudent insured should involve the insurer in any adverse cyber event and utilize the insurance-company's preferred vendors.[22] The objective is to make it easy for the insurance company to write checks.

[22] Questions of confidentiality and privilege usually can be navigated, but should be considered expressly.