May 3, 2024

PRACTICAL CYBER INSURANCE FOR UNIONS

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

Labor unions, like other 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 2022 there were some 629 different insurance companies selling cyber 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

[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 teaches insurance law at George Washington University Law School (for more than 20 years) and 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.

[2] National Association of Insurance Commissioners, *Report on the Cybersecurity Insurance Market* (Nov. 3, 2023)

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 50 percent of the market, with the top 25 constituting 86 percent of the market (by premium collected).[3] The need for cyber insurance has led to a burgeoning market.

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, even for small 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,

---

[3] According to the Federal Insurance Office Annual Report on the Insurance Industry (Sept. 2023) at 45, the top ten in order of premiums collected were:

Chubb Ltd
Fairfax Financial Holdings Ltd.
AXA SA
Tokio Marine
Arch Capital
Travelers Companies, Inc.
American International Group (AIG)
Nationwide
Zurich
Sampo

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 https://www.verizon.com/business/resources/reports/dbir/2023/summary-of-findings/ Even considering the advance in machine learning and artificial intelligence that empower hackers further, human factors and failure of employees to abide by cybersecurity protocols contribute to virtually all cyber losses. *See* https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html ("even the most advanced data breaches with AI enhanced spear phishing will still involve the human element in approximately 90% of instances").

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

[6] *Id.* at 10. In one publicized instance, a union chose not to pay the ransom and instead rebuilt its systems from back-ups.

effectively doubling the total loss, in recovering its operations.[7] According to one source, ransomware payments are averaging nearly $400,000, with the ransom demands exceeding $1.6 million.[8] Another source says that average ransomware payments in the third quarter of 2023 averaged $568,707, with 2024 showing even more attacks than did 2023.[9]

Ransomware is introduced via a phishing email[10] or via recently discovered "exploits" or design defects in software that permits hackers to gain access.[11] In some instances, ransomware involves exfiltration of data, with the hackers threatening to release the data if ransom is not paid (in addition to locking the organization out from its own computer systems). And ransomware as a vector for anti-union political action is conceivable, suggesting that the social-political environment could make unions more of a target for bad actors.[12]

> Communicating with Teamsters officials on the dark web through a site provided in the ransom note, the attackers demanded $2.5 million in exchange for restoring the union's access to electronic files. Personal information for the millions of active and retired members was never compromised, according to a Teamsters spokesperson, who also said that only one of the union's two email systems was frozen along with other data. . . . [Teamsters] Union officials in Washington were divided over whether to pay the ransom — going so far as to bargain the number down to $1.1 million, according to the sources — but eventually sided with their insurance company, which urged them not to pony up.

https://www.nbcnews.com/tech/security/ransomware-attack-hit-teamsters-2019-they-refused-pay-n1270461.

7 Hiscox, at 11.

8 https://www.coalitioninc.com/blog/2023-cyber-claims-report-update

9 https://www.blackfog.com/the-state-of-ransomware-2024/

10 "Phishing" should be understood to include: email phishing; "spear" phishing using personalized information; voice phishing or "vishing" that uses deepfake voices; SMiShing of SMS messages; and fake QR codes ("Quishing").

11 https://www.chainalysis.com/blog/ransomware-2024/

12 In the UK, the Public and Commercial Services (PCS) Union website was knocked offline through a denial-of-service attack that coincided with consideration of a strike vote in May 2011.

The theft of "personally identifiable information" or "personal health information" that is maintained by an organization may or may not be accompanied by a ransomware demand. Sometimes, the objective for the mal-actors is the data maintained by the organization.[13] Anti-union employers (or their agents) may seek to identify union members for retaliation, and outside groups (or individuals) with political or other animus might seek private information, such as a member's affiliation with an internal LGBTQ+ group.

A key computer-based risk concerns "funds transfer fraud" or sometimes referred to as "social engineering fraud."[14] This occurs when the organization is tricked into sending monies; these losses also arise when the bad actor accesses an online banking portal or treasury-management system through theft of passwords and the like. As of mid-year 2023, the average loss was close to $300,000.[15] Often, the bad actor "dwells" in the system for more than a month (having gained access initially via a phishing email), and then spoofs or hijacks internal or external communications to direct a change in instructions for invoice payment. By impersonating an executive, vendor, or bank, or by sending falsified or fake invoices or payment instructions, the organization is tricked into making payment.[16]

---

[13] https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf

[14] Some insurers categorize "funds transfer fraud" to occur without the knowledge or involvement of someone at the insured organization but rather involves the theft of passwords or access to a treasury-management system. Such insurers then add the category of "social engineering fraud." Also, some fund-transfer fraud losses may be covered under separate "crime protection" and fidelity policies depending on the wordings. *E.g.,* Valero Title Inc. v. RLI Ins. Co. (5th Cir. 2023), available at https://www.ca5.uscourts.gov/opinions/unpub/22/22-20155.0.pdf

[15] https://www.coalitioninc.com/blog/2023-cyber-claims-report-update

[16] Fraudsters are using artificial intelligence and related tools to spoof participants in virtual meetings, and such voice and video impersonation can be expected to increase. *E.g.,* https://www.ic3.gov/Media/Y2022/PSA220216. In a year-end summary, one group observed, "cybersecurity researchers increasingly point to anecdotal evidence of identity criminals pairing stolen personal information with Generative AI tools. The result is highly effective phishing and social engineering attacks that target specific businesses or individuals rather than the traditional phishing lures that were riddled with grammar errors and launched with little knowledge of who was receiving the message." https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf at p. 10. As technology marches forward, so too do the schemes:

> Since AI tools and deepfake technologies have become part of the mainstream criminal's toolbox, convincing fake phone calls or digital

Because of the frequency and severity of computer-based losses and the proliferation of various state statutes addressing consumer privacy and data breach, courts and regulators require entities and their leaders to protect the organization from cyber-losses.[17] The Department of Labor's Employee Benefits Security Administration on April 14, 2021, issued three cybersecurity guides: "Tips for Hiring a Service Provider[18]," "Cybersecurity Program Best Practices[19]," and "Online Security Tips.[20]" This follows the Department of Labor's Office of Labor-Management Standards' "Special Advisory" on "Labor Organization Emergency Preparedness" in July 2020, which provided "suggestions" and "strategies" regarding technology updates, including among other things:

- Establish remote access to union software containing membership data that ensures the safety and security of this private information.

- Consider using a document management system that allows records to be stored in a cloudbased format. Any systems used should ensure adequate cyber-security.

- Consider using two factor authentication on union accounts – i.e. if an authorized signatory needs to make an electronic payment a code would be texted to the other authorized signatory.

> meetings as well as videos are broadly and cheaply available for scams. In early 2024, a Hong Kong based employee of a multinational company transferred nearly $26 million to scammers after attending a video call with deepfakes of their co-workers, including the company's CFO. The employee was the only human being who attended the video call, while fake participants were impersonated with AI-driven technology.

https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html

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

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

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

[20] https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/online-security-tips.pdf

- Ensure that you create adequate backups of documents and systems.[21]

Today, a robust computer-security program will include the purchase of cyberinsurance. In part, the "cyber hygiene" requirements to qualify for cyber insurance provide useful guides to check the cyber-security status of the organization. Many insurers as part of underwriting run "penetration tests" on the existing systems to assess how well armored the potential insured's systems are.

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.[22] For many, the bundle of free, included, or discounted services that come with a particular policy alone make the purchase of cyber-insurance worthwhile.[23] Upon purchase (or "pre-breach"), the insured will have access to resources such as free publications, free or discounted software or services, and recommended best practices, including materials, software, or vendors regarding:

1. Incident Response Readiness
2. Security Awareness
3. Information Governance
4. Security Risk Ratings
5. Cyber Security Standards
6. Encryption
7. User Access Controls
8. Regulatory and Standards Compliance
9. Password Management

---

[21] https://www.dol.gov/sites/dolgov/files/olms/regs/compliance/comp_pubs/EmgPrep_Special_Advisory_July2020.pdf

[22] 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).

[23] *See*, *e.g.,* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses*, Law and Social Inquiry (American Bar Foundation 2017).

In the event of a cyber "incident" or cyber "breach,"[24] insurers will often provide a dedicated "breach coach," and access to preferred vendors to provide response services including for:

a. Computer Forensics
b. Public Relations
c. Notification and Identity Services (such as credit monitoring)
d. Call Center Services
e. Cyber Extortion and Ransom Services
f. Legal and Regulatory Communications
g. Business Interruption (Operation Recovery) Services

In some insurance policies, the insured may use other vendors with the insurer's consent; in some policies, deductibles are waived or reduced if the insured uses the preferred vendors; in some policies, no coverage is provided for "out of network" providers chosen by the insured.

Although following a major loss it behooves the insured to explore recovery under any available insurance,[25] the focus of in-house lawyers and outside counsel

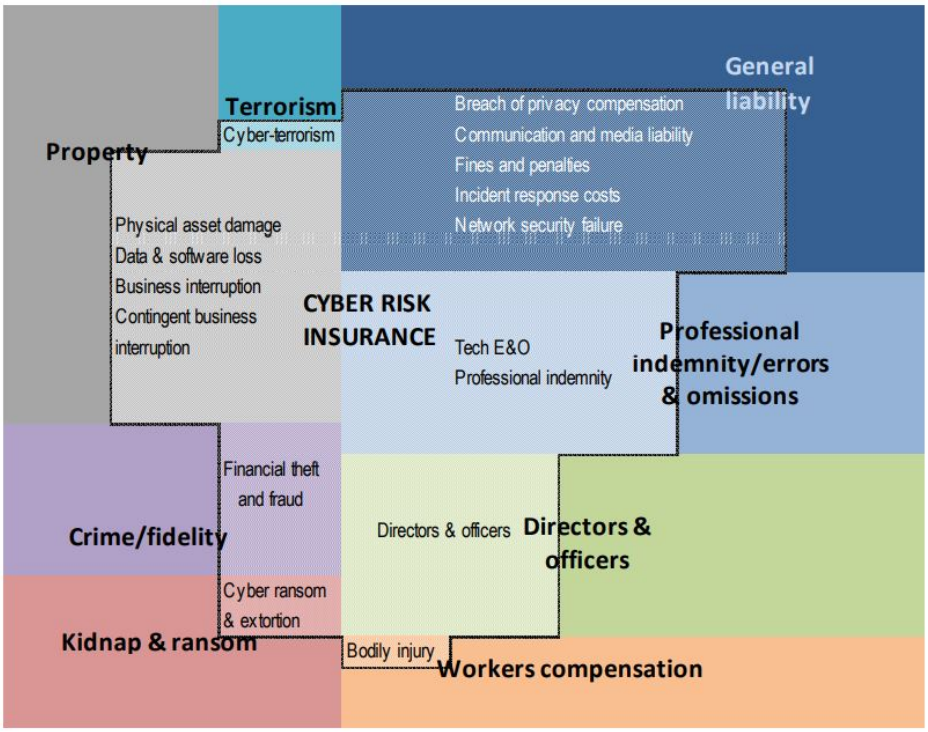
[24] The term cyber breach refers (properly) to an event involving exfiltration or theft of data; other cyber-related events are termed "incidents."

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

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 may not be of great value to labor unions and affiliated organizations, but are included in the standard offering of the more than 600 insurance companies in this market.[26] Absent some unique exposures, for the most part unions do not need to focus (much) on the following coverages in a proposed cyber policy:

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

[26] As one academic study observes:

> 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.

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.

In general, policies do not cover pre-existing cyber events, improvements to systems, or failure to address known vulnerabilities.

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). Unions and affiliates routinely maintain records about their members, some of which may be subject to newer privacy regulation.[27] Such stray personally identifiable information if exposed to hackers may trigger statutory notification requirements. Indeed, one union is presently being sued in several class actions concerning a breach from late 2023 exposing records of names, social security numbers, driver's licenses, state identification numbers, alien registration numbers, tribal identification numbers, passport numbers, birth certificates, dates of birth, marriage licenses, signatures, financial account information, and medical information. The same union was required to file in several states a publicly available notice of data breach, including estimating the number of state residents potentially affected.

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

[27] 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.

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, and the frequency of ransomware attacks are expected to increase.[28] In a ransomware attack, users are locked out of all or part of the organization's computer system.[29] According to a recent survey, in more than two-thirds of cases, the victim pays ransom; sometimes they pay ransom more than once.[30] Sophisticated ransomware attacks include partial disclosures by the perpetrators of damaging information and contacting customers directly to taunt the victim. The increasing profitability of this criminal enterprise and the increasing availability of ransomware-as-service and of hacking toolsets underscores that any organization can fall victim to a ransomware attack, as several local, national and international unions have found. The most likely vector is a phishing email that installs malware on the network but direct 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.

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

---

[28] *E.g.,* https://www.munichre.com/en/insights/cyber/cyber-insurance-risks-and-trends-2024.html "The Munich Re Cyber Data Analytics Team observed that ransomware was, by far, the leading cause of cyber insurance losses."

[29] 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

[30] *Hiscox Cyber Readiness Report 2021.*

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, often through "business email compromise" or "business communication compromise" and phishing. 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 "funds transfer fraud," "cyber crime," "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.

Some policies expressly condition coverage on the insured's following its own proper (and approved) procedures for funds transfers, such as separate verification of identity of the recipient. Depending on the policy, the language might be read to exclude coverage for the negligent failure to follow such internal procedures. As an example:

> "[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."

The organization whose policy includes such language should ensure its everyday internal processes conform.

4. Failure to Update, Patch Software Exclusions

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]."

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.[31] (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.[32]

---

[31] In *Columbia Casualty Co. v. Cottage Health System*, 2:15-cv-03432 (C.D. Cal. May. 7, 2015), the insurer sought a ruling that it did not cover class action data-breach lawsuit. The class action alleged the insured failed to take security measures to protect medical records from becoming available to via the internet. The insurer purported to rely on a "Failure to Follow Minimum Required Practices" exclusion —which precluded coverage for failure "to continuously implement the procedures and risk controls identified in the Insured's application." Among other things, the insurer alleged the insured failed to:

- Replace factory default settings to ensure that its information-security systems were securely configured;
- Regularly check and maintain security patches on its systems; and
- Exercise due diligence with respect to its information-security-management vendor's safeguards.

[32] In one case, Travelers sought rescission of an insurance policy it issued on the ground that the insured was not in compliance with its representations in underwriting about its cyber-security practices (in particular, its use of "multi-factor authentication"). The case was dismissed soon after it was brought. *Travelers Property Cas. Co. v. International Control Services, Inc.* (C.D. Ill. 2022).

Not all policies include such exclusions. If such an exclusion is accepted by the insured, it needs to ensure that it can document ongoing compliance to avoid dispute later when a cyber-event 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.[33] 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.

---

[33] *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.

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.[34] 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.)

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. The objective is to make it easy for the insurance company to write checks.

---

[34] Whether all communications following a data breach or cyber incident are cloaked in attorney-client privilege and attorney work product is highly disputed. *See* https://netdiligence.com/blog/2021/10/attorney-client-privilege-in-cybersecurity/ Probably the key case that highlighted the issue was *In re Capital One Consumer Data Security Breach Litigation*, No. 19-2915, 2020 U.S. Dist. Lexis 91736 (E.D. Va. May 26, 2020). Questions of confidentiality and privilege usually can be navigated, but should be considered expressly.