

Maximizing Cyberinsurance Coverage In 2026

By **Marc Ladd and Alexander Sugzda** (January 6, 2026)

One of the most significant risks policyholders face in 2026 is the risk of loss caused by infiltration of their computer systems or manipulation of their employees through the use of computers.

Bad actors such as hackers and fraudsters target both large, sophisticated companies with cyberattacks in the pursuit of huge monetary transfers, and small businesses in the hopes that their systems are more easily hacked, or their employees are more easily manipulated to provide confidential information.

Not only are these cyber events becoming more common — it is also becoming far more difficult to track the bad actor, meaning that cyber insurance is becoming more and more important as a significant source for reimbursement for these bad acts.

And while claims for coverage for social engineering and fraudulent fund transfer by bad actors are becoming more prevalent, it is important to remember that cyberinsurance should cover unintentional computer system loss as well, such as a network disruption and data leaks. Every policyholder should evaluate the options for cyber coverage and be prepared to maximize coverage in the event a claim arises.



Marc Ladd



Alexander Sugzda

Reviewing the Scope of Cyberinsurance

Many cyber policies may appear to provide broad coverage based on the number of coverage grants included in the policy. For example, some cyber liability policies will have the policies' general terms and conditions that apply to all coverages (unless provided otherwise) and contain important information such as what constitutes a "claim" for notice purposes, and how and when to give notice after you have suffered a loss.

Indeed, there are sometimes six and seven different coverage grants provided under the same insurance package, including coverages for cyber-extortion, system hijacking, counterfeit currency fraud and even invoice manipulation.

That being said, the cyber policies being written today are thoroughly drafted, include far more defined terms, and are more complicated than the standard general liability and directors and officers liability policies, where the most a policyholder needed to establish coverage was simply an "occurrence" or an alleged "wrongful act," respectively, to trigger coverage.

Overlapping Definitions

For example, a policy that provides cyber coverage may respond when the policyholder suffers a loss through a system hack — but the policy likely will require much more than just that fact to be triggered.

Certain cybercrime coverages require more than just a crime and a computer; to be

triggered, there must also be a "direct loss" by the policyholder's "parent organization" of "money or securities" resulting from "computer fraud" committed by a "third party." On its face, the coverage can seem straightforward; however, each quoted term is a defined term that often contains additional defined terms that then depend on additional defined terms.

The required "computer fraud" mentioned above is defined as the "unlawful taking of money or securities" resulting from a "computer violation," which in turn means, inter alia, the "fraudulent ... change to data elements or programmic logic of a computer system," where "computer system" is defined as ... well, you get the picture.

All of this does not even include coverage intended for loss from "social engineering fraud" that requires that a person purporting to be a "vendor," "client," or an "employee" and intentionally misleading through material misrepresentation. Simply trying to follow the trail of definitions — that often refer back to each other — can lead the policyholder down a wormhole trying to figure out which coverage may apply.

Policyholders must review the terms of any policy being proposed — especially the endorsements that can completely reshape the insurer's cyber form.

Overlapping Coverages

In addition to overlapping definitions, cyber policies can also include overlapping coverages as underwriters try to write ever-changing risks. A cyber coverage policy may include four separate insuring grants for "network security," "cyber extortion," "social engineering" and "computer fraud," each with its own separate limit of coverage, and all of them triggered by the same loss and the same set of facts. However, the limits for most of these coverages remain relatively low for companies (\$150,000 to \$5 million maximum).

As such, before accepting a cyber policy, the policyholder should try to obtain cyber coverage where the limits are cumulative, i.e., they can be stacked for each triggered coverage. Try to avoid a policy that limits the amount of coverage solely to the largest coverage grant triggered.

When the policyholder suffers a loss and wants to provide notice, the notice should be as nondescript as possible regarding the potentially triggered coverage so as not to box-in recovery to only one potential coverage. Instead, provide the facts and allow the insurer to state first which coverages apply (and which do not) and why, which the policyholder can then rebut if necessary.

The Current Evolution of Cyber Coverage

Even though cyber coverage has been around for almost 30 years, it is still a relatively new risk being insured as compared to fire loss or marine hull, which have been around for hundreds of years and still employ a standard form.

Underwriters and brokers are still finding their footing when trying to match the language to the scope and type of risk, and that becomes even more challenging as technology continues to move at a rapid pace. Naturally, when the underlying risks expand and evolve as much as they do in cybersecurity, the language covering those risks must adapt or find itself obsolete.

Coverage for social engineering provides a case in point on the evolving nature of cyber coverage. Social engineering fraud, which includes email spoofing, is now a popular form of

cybercrime and involves the use of deception to manipulate individuals into divulging confidential, financial or personal information.

However, when these scams began to proliferate about 10 years ago, crime and cyber coverages did not have a "social engineering fraud" defined term or separate coverage at all. But because the facts of the loss could fit within the policy's computer fraud coverage, policyholders were able to succeed on email spoofing claims under those coverages.

The insurance industry swiftly responded to these, and soon many coverage forms were amended to define social engineering fraud and either excluded it altogether or subjected it to lower sublimits than other crime or cyber coverages. Corporate policyholders purchasing cyberinsurance in 2026 should be aware of whether coverage for social engineering fraud is excluded by their policies and seek to have it added with the highest possible limits, as often the losses for these cyberattacks far outstrip the low sublimits insurers initially offer to policyholders.

Today, insurer underwriters are continuing to evaluate newer risks to insure as part of a cyber package offered to potential policyholders.

These include coverages for ransomware, bodily injury or property damage that arises out of a cyber event — for example, a cyberattack that shuts down a building's security system that leads to third-party vandalism — and even coverage for losses to or caused by a company's artificial intelligence activity, which is becoming more prevalent.

However, insurers have been just as active in making sure they are limiting these coverages along the way, either by exclusions or by refusing to write significant limits, given the inherent difficulties in predicting cyber risk. Accordingly, policyholders still may have to resort to more creative arguments to recover on a significant cyber loss.

Maximizing Coverage for Cyber-Related Losses

Indeed, despite its constant evolution, there will still be instances where the policy's cyber coverage has not yet caught up to the technology it is supposed to cover. In these cases, where a cyberinsurance coverage grant or policy is potentially not triggered due to its limited scope or burdensome requirements, or perhaps is only covered for low limits, a policyholder should review its additional policies' coverage grants that may provide a backdoor recovery for cyber loss.

Policyholders may want to consider obtaining multimedia coverage that can be purchased separately but can also be included in the cyber policy, which can provide generally higher limits and soft spots in coverage for computer-related crimes. Another example is an insurer's packaging for an executive protection portfolio that includes the mainline directors and officers coverage, but also contains coverages for crime, forgery, or funds transfer fraud, which encapsulate the facts of a cyber event.

For example, "funds transfer fraud" has been written to provide coverage for "fraudulent electronic ... instructions purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent."

Even though the portfolio does not include social engineering or spoofing coverage, the definition above spells out coverage for a social engineering-like loss. And even where the

policy has a specific endorsement excluding coverage for social engineering loss, the above definition of "funds transfer fraud" would create an ambiguity that should be read in favor of coverage for the policyholder.

Accordingly, to the extent that a cyber coverage part does not apply, is not offered, or is not offered with any significant limits, before deciding to not pursue any coverage for the loss, the corporate policyholder should review its other policies to determine whether any provide coverage for cyber-related losses.

Moreover, policyholders should also be attuned to the potential for inconsistencies in package-type policies that could result in the availability of additional limits to pursue. A package policy that provides both crime and cyber coverage could include separate limits that both apply for the same loss.

Conclusion

Policyholders in 2026 should pursue broad-based risk management strategies to avoid or mitigate cyber losses.

They should protect their systems and train their employees to prevent such losses and stop them as fast as possible; the longer a cyber event goes, the larger the exposure.

If losses do happen, policyholders should have the best possible insurance in place as a backstop — this may include obtaining coverage from multiple carriers to achieve the highest possible limits available in the market and getting broad, overlapping coverages with limits that can be stacked. Cyber policies can confuse corporate policyholders with their constantly evolving terminology and dizzying array of definitions that contradict each other, but they provide a valuable asset following a cyber event.

Marc T. Ladd and Alexander M. Sugzda are partners at Cohen Ziffer Frenchman & McKenna.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.