SHUTTERSTOCK/STOKKETE

WHAT'S IN A WORD?

The Hidden Pitfalls of Cyber Insurance Policy Language

BY BERT WELLS AND JEFF KIBURTZ

While cyber insurance policies have been standard fare for many companies for at least a decade, challenges with policy language continue to emerge and evolve. One such issue relates to properly identifying the insured's IT systems. Although by no means a new concern, shifting policy language and rapid adoption of new IT architectures have created prime conditions for misunderstandings between policyholders and their insurers. This problem often boils down to whether a defined term in the policy such as "computer system" encompasses all of the IT resources that the policyholder uses in its business. Too often, there is a gap between a business's actual IT operations and the policy language specifying the limits of covered data, software and hardware.

To help minimize the possibility of coverage disputes due to a disconnect between the cyber policy's language and actual IT operations, policyholders, and the insurance brokers and lawyers who advise them, should carefully study the relationship between policy wording and the ever-evolving technical circumstances of the business's IT operations. Potentially at stake is an expensive coverage dispute or worse yet, a clear-cut coverage gap for some of the policyholder's IT resources.

The wide range of cyber policy language—which can vary greatly among insurers—and the even wider range of possible IT operations precludes a detailed discussion of these issues. But several general principles may help prevent a potential coverage gap.

The Changing Structure of Corporate Data Processing

A key source of potential gaps or misunderstandings has been the rapid pace of IT development and deployment. Few, if any, sizeable businesses rely only on the computers, servers and other hardware in their own physical possession on their own premises. Ubiquitous high-speed data communications and decades of advances in software and hardware technology have radically changed where and how companies' IT needs are met, enabling business practices such as:

- Relocating computers to off-site locations where they are accessed via the internet;
- Contracting with software-as-a-service (SaaS) providers to avoid the need to download software necessary for their business;
- Storing and processing data via cloud service providers whose IT architecture may be so dynamic that data has no long-term fixed location and the hardware platform processing it may not even be identified or allocated until the need arises; and
- Bring your own device (BYOD) programs that rely on employees using their own mobile devices.

In particular, cloud computing and virtualization technology are increasing the physical distance between users and the hardware and software on which they rely. A customer can, for example, contract with a vendor to interact via browser with remote hardware running software that emulates the experience of controlling a desktop computer or server. The customer can then store data on this virtual machine, obtain commercial applications to run on it, and develop and run custom software, all with the same ease and control as if wired to a company-owned computer in the next cubicle.

In other words, the IT systems that once might have been readily identifiable at a particular physical location within the policyholder's premises may now be part of a larger ecosystem of hardware, software and data widely distributed among multiple locations in both physical space and online, all potentially vulnerable to cyber intrusions or compromise.

How IT Operations Structure Affects Coverage

Policyholders may not fully appreciate the impact such technological transformations can have on their cyber policies. They generally expect cyber insurance to protect them from both accidental and malicious interference with their IT operations. But because cyberrisks can materialize anywhere in the IT ecosystem on which a company's operations rely, they need their policies to cover the full range of those operations, regardless of where those resources are physically located.

Insurers, on the other hand, craft policy language to confine their own exposure to IT operations that they deem within a safe zone of underwriting. Some may deem cloud computing, virtual servers and SaaS to fall outside that zone. The resulting policy language may fall short of encompassing the full range of IT operations that the policyholder could reasonably expect would be covered.

Accordingly, a central issue when first procuring or renewing cyber insurance is how the proposed policy specifies the scope of the insured portions of the policyholder's IT operations. Cyber policy forms vary by insurer, but typically address this issue through a defined term such as "computer system," "insured's computer system" or "insured's system." Far more significant than cyber insurers' differing terminology, however, are the different ways they define the "computer system" concept, and thus the extent to which their policies cover the assemblage of data, software and hardware, on-premises and off, upon which a policyholder relies.

Most cyber policy definitions of "computer system" contain three basic elements: 1) the covered types of IT assets (i.e., various types of data, software and hardware); 2) the relevant entity or entities for establishing an insurable relationship or nexus to the assets, which always include the insured and usually certain qualifying service providers of the insured; and 3) the nexus language stating the kind of relationship the insurable IT assets must have to the relevant entity. The following subsections of this article probe each of these three elements.

However, as an additional word of caution about an extremely confusing aspect of interpreting many cyber policies, the definition of "computer system" can vary within a single policy according to which cyber coverage grant is at issue. For example, an outsourced server covered for purposes of data breach response might not be covered for loss resulting from a denial-of-service or ransomware attack.

Covered Types of IT Assets. Although the word "computer" is almost always used in cyber policies, it is not always a defined term. Some policies may mention "computer hardware," a term that likely conjures images of physical devices such as servers, desktop computers, laptops, circuit boards and other macroscopic, tangible platforms for computing. Other policies, however, provide few clues as to whether the parties intend "computer" to refer only to such tangible devices or also to the software that actually provides the computing function. This distinction can be critical depending on the degree to which the policyholder uses virtualization technology. An insurer might argue, for example, that "computer" refers only to the physical hardware and not a virtual server, regardless of whether the policyholder relies just as much on virtual servers as physical servers.

In addition to computers (defined or not), many policies define "computer system" to expressly include the most familiar types of IT assets, such as elec-

tronic data, software programs, electronic data processing hardware, mobile electronic computing and communications devices, data storage devices, and networking equipment. Policyholders should not only confirm that the most valuable or vulnerable aspects of their computer systems are included on the list of covered resources, but also that no overly narrow terms—and nothing in the policy as a whole—might inappropriately limit the categories of covered IT resources.

Relevant Entities for Determining Insurable Relationship to IT Assets. The next key concept in defining the insured property is to identify the insureds or other relevant entities that own, operate or otherwise have the required relationship to the IT assets for which the policyholder expects coverage. These third parties, which we will refer to as "qualifying IT entities," may themselves be the subject of separate definitions in the cyber policy. In some cyber policies, qualifying third-party IT entities are limited to the direct providers of IT services to the insureds. In others, the third-party entities may include any other provider on which a policyholder depends. Accordingly, careful parsing of policy language is usually required to determine which potential off-premises cyber incidents will be protected (an analysis that, like the definition of "computer system," may vary by coverage part).

That determination can be challenging for even small companies due to the various computing architectures that a single user or business unit may deploy, including BYOD programs. For large organizations, the effort to vet the range of qualifying IT entities compared to the policyholder's operations can be extremely complicated, but it is critical.

There are two particularly common failings in policies' approaches to qualifying IT entities. The first is imposition of overly restrictive conditions for providers to be qualifying IT entities. Even a seemingly minimal (and common) condition that IT services of a qualifying IT entity be provided pursuant to a written contract might present coverage questions about cyber incidents that originate indirectly, such as with subcontractors of direct vendors. A written condition might also prompt a dispute over whether a vendor providing ancillary IT services qualifies.

Consider, hypothetically, a parts supplier that hosts an electronic inventory and ordering system essential for a manufacturer's timely procurement of parts. The only written contract between the two might be a purchase agreement that is silent about the electronic system. A cyberattack on the parts supplier could halt the policyholder's supply chain, causing business interruption loss. But if the policy requires that a qualifying IT entity's IT services be pursuant to "written contract," the insurer might try to argue that this cyber-related loss is not covered.

A second common failing is that a policyholder's cyber policy might omit a corporate affiliate that supports some critical aspect of the policyholder's IT operations. Consider, for example, a multinational company that outsources critical U.S. accounting functions to a subsidiary in India, but insures non-U.S. affiliates under foreign-issued policies instead of a unitary global cyber policy. Depending on policy terms, the result might be no coverage, or coverage disputed between the U.S. and Indian insurers, for a U.S. loss resulting from a cyberattack on the Indian operations.

Thus, ensuring that a proposed cyber policy includes the appropriate entities as qualifying IT entities should be a core focus of cyber policy analysis, because any gaps may create a large category of uninsured IT operations. Furthermore, the policyholder might discover simple ways to eliminate certain gaps. In the first example, they might revise the purchasing agreement to refer to the electronic ordering system. If the policy is not scrutinized for such conditions on qualifying IT entities, however, the full potential benefit of the coverage may not be achieved.

Relationship Between Qualifying IT Entities and Covered IT Assets. Cyber policies typically define the required relationship between the qualifying IT entity and the IT asset for which coverage is granted by using one or more terms such as "owned," "operated," "leased," "licensed," or "controlled," and occasionally require such forms of dominion to be "exclusive." Policyholders should be particularly vigilant in vetting this kind of terminology.

One common issue is that the verbs used may not match the policyholder's operations. For example, if a policyholder licenses certain software or data, but the "computer system" definition refers only to owning or leasing IT assets, then an insurer might argue that losses resulting from damage to licensed software is excluded from coverage. The policyholder would likely argue, among other things, that it owns its copy of the software and that this type of ownership suffices for coverage.

A second common issue is that many words typically used in this context, such as "operate," "lease" and "control," can be unclear in practice. For example, outsourced IT resources commonly require the combined efforts of two or more parties, like when one party, an IT service provider, supplies power, cooling, internet connectivity, an operating system and security patches to a physical server, while the other party, the policyholder, conducts the useful data processing on that server. Not every insurer will resolve in the policyholder's favor which party or parties should be deemed to "operate" or "control" such a server. Of course, in litigation or arbitration, a legal presumption that any ambiguity in the policy language should be construed against the insurer might apply.

Accordingly, any policyholder should

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com

carefully scrutinize the nexus terms in a proposed cyber policy to ensure that they reflect all of the relationships between the policyholder's qualifying IT entities and the IT assets that the policyholder expects to be covered.

Reviewing the Entire Policy

Although "computer system" is a key defined term that can either remedy or create coverage gaps, a broad definition alone does not guarantee that coverage will be available for every incident affecting IT assets within that definition. Rather, insurers may deploy a number of other provisions to limit coverage scope. Accordingly, cyber policies must be read as a whole, with attention to how one part may affect another.

On the other hand, not every coverage part of a cyber policy necessarily relies on the "computer system" definition. Privacy breach response coverage, for example, is often independent of how or where the compromised private information was stored. Indeed, it is typical for data breach response coverage to be triggered by the compromise—whether by theft or other loss—of personal information recorded on the policyholder's paper documents, as well as electronic records and any other records for which the policyholder is legally responsible.

Regardless of these caveats, in view of the dynamism of commercial IT operations and architecture, the definition of "computer system" has become a logical focal point for evaluation of any proposed cyber policy. Policyholders, and the brokers and lawyers who represent them, must assess that definition with care and with the fullest possible understanding of the policyholder's IT ecosystem. ■

Bert Wells is a partner at Covington & Burling LLP, where he represents policyholders as part of the firm's global insurance recovery practice. **Jeff Kiburtz** is Of Counsel at Covington & Burling LLP, where he represents policyholders as part of the firm's global insurance recovery practice.

RISK MANAGEMENT

Reprinted with permission from Risk Management.

www.rmmagazine.com