Protecting the professionals

What's changing when it comes to exposures confronting directors and officers – and those they employ?

THE WORLD continues to evolve, and so too does the range of exposures that corporate entities and their employees face.

As the pace of change increases, it's imperative to understand the shifting landscape and the must-have coverages for professionals. *Insurance Business America* spoke to industry experts about a range of issues impacting a number of key products within the professional liability suite.

Directors & officers liability

Reflecting on the regulatory landscape, Alex Jezerski Jr. of RT ProExec says the most worrisome trend facing directors and officers this year is the continued vigilance of the US government in holding those individuals accountable for corporate wrongdoing. Specifically, Jezerski refers to a memo circulated by Deputy Attorney General Sally Quillian Yates to all Department of Justice attorneys last September, commonly referred to as the Yates Memo.

"The US Department of Justice has made it very clear that if a company wishes to qualify for cooperation credit in connection with a DOJ investigation, the company must be forthcoming with all facts related to any individuals involved in the alleged misconduct," Jerzerski says.

He adds that the US Securities and Exchange Commission also remains sharply focused on targeting individual directors and officers in its enforcement actions.

"In addition to going after fraud and overt misconduct, the SEC is seeking to hold directors and officers accountable for inattention and failure to follow acceptable corporate governance protocols," Jerzerski says.

Matt Sheehan, senior vice president of financial services for Worldwide Facilities, says the potential impact of the Yates Memo is something he's discussing with clients.

"I think the burden of proof to go after individual directors and officers and managers of companies is going to be lessened, and it's going to be a more common strategy for regulators," Sheehan says. "When regulators go after individuals and their business decisions, the plaintiff's bar takes notice. Usually, there's litigation to follow."

Sheehan also highlights the rising number of actions under the False Claims Act, targeting companies attempting to defraud the US government.

"If a director is running a business that provides services or products to the US government, the likelihood that an investigation or action [will be] brought against them is certainly heightened," he says. "Most people think that that's just in healthcare billing and reimbursement, but we're seeing

"In addition to going after fraud and overt misconduct, the SEC is seeking to hold directors and officers accountable for inattention and failure to follow acceptable corporate governance protocols"

Alex Jezerski Jr., RT ProExec

WHAT IS D&O LIABILITY?

Directors & officers (D&O) liability insurance protects boards of directors and officers of organizations (which can include companies, nonprofit organizations and educational institutions) against claims of alleged wrongful conduct while acting as directors and officers.

it across private entities that provide services to the government."

Sheehan says another regulatory shift gaining momentum is the use of the Americans with Disabilities Act to pursue actions against website operators.

Blind or deaf people need reasonable accommodations to a public website, should it be closed captioning or audio descriptions of pictures or help in entering credit card information," he says. "So companies are spending a lot more money to make their websites accessible to all. But we are seeing plenty of actions along these lines, and the plaintiff's bar has taken notice."

As for what separates the best D&O liability products in the market from the rest, Jezerski emphasizes the importance of structuring the policy to provide appropriate coverage for government actions and investigations.

"Generally speaking, D&O policies have improved steadily in this regard since 2010," he says. "But there are still significant differences in coverage from policy to policy."

Sheehan advises watching out for anti-trust exclusions. "Claims by competitors in the United States tend to be fertile ground for D&O claims in the private company space, and the absence or addition of an anti-trust exclusion is a big differentiator," he says. "We saw carriers pull back on that in the past couple of years.

"The defense costs allocation provision in a private company form is also very big," he adds. "If a portion of a multiple-allegation claim is covered, there still are a vast number of carriers that will pay 100% of defense costs for an individual insured, which is a tremendous luxury to the insured – not only in not having to pay those costs, but also setting a defense strategy that makes sense because they aren't trying to get out of it for a minimal cost. They have time to actually formulate a strategy that makes sense for the long run for them and their business and their reputation."

Sheehan believes that, in the coming years, pre-claims assistance will also differentiate D&O products.

"We have a lot of carriers that try to not call a letter or a demand a 'claim' so they can avoid providing defense costs, which is the opposite of what we want them to do and the opposite of what they want to do, I think," he says. "I think it would be better for them to just affirmatively cover pre-claim defense costs where they can get in early, set a strategy, and do some preliminary discovery or fact-finding that's going to help their case, both helping the insured and the insurer.

"I would expect insurers to come out with affirmative pre-claim assistance and really enumerate the services that they will provide. It will encourage insureds to report claims faster, as well as, I think, it'll just sell in the marketplace, and the insured's and the carrier's interests are aligned in this area. So I would expect more robust endorsements to manifest themselves."

WHAT IS E&O INSURANCE?

Errors & omissions [E&O]insurance protects professionals against negligence claims and claims of failing to perform (or making an error) in providing their professional advice and services.

"As large technology companies move into new areas of services, they often encounter legal issues that are new and untested. This is a trend that will only continue"

Mickey Estey, RT ProExec

PROFESSIONAL LIABILITY

Errors & omissions

Which professions should pay extra attention to their E&O exposures in 2016?

"Large technology companies continue to see many unique claims and will be paying extra attention to exposures related to data privacy, cyber attacks, the Telephone Consumer Protection Act, social media content and intellectual property," says Mickey Estey of RT ProExec.

"We are seeing this reflected in the increased insurance limits purchased by many technology companies," he continues. "With so many technologies being provided on a cloud basis, the exposures are significant for both the large technology companies providing those services, as well as the businesses that are relying on those services on a growing basis for those core functions. As large technology companies move into new areas of service, they often encounter legal issues that are new and untested. This is a trend that will only continue."

Sheehan cites oil & gas consultants as another category of professionals who should contemplate a heightened focus on their E&O exposures. "Any sector that's had a downturn … generally is going to see a spike in claims activity because people are looking for the deep pocket. The oil & gas industry generally is full of speculators with a healthier risk tolerance, and they're generally not litigious. But we would figure that, at some point, some of these bankrupt entities may look to point the finger. Even if the business owner that failed is not ready to point the finger, some bankruptcy estates may do so."

Beyond oil & gas, Sheehan talks about investment advisors, who will be affected by a new Department of Labor fiduciary rule.

"There's stronger language in that fiduciary rule that those individual advisors have to represent the client's best interests and they really need to show that there's not a conflict of interest by putting an investor in an investment with a higher cost structure and higher fees in it," he says. "With that rule coming out, one can only assume that the plaintiff's bar is going to take notice. They usually follow the regulators and find negligence within those rules and pursue private courses of action. I think a lot of folks in the investment community and the retirement planning benefits community are taking notice and trying to provide proper communication to avoid regulatory action and lawsuits."

And then there's contractors' E&O. "More and more, we're seeing contractors being required by contract to carry contractors' E&O," Sheehan says. "With the way projects are delivered now, and the sophistication of the documentation software while delivering a construction project … there's always direction and advice coming from contractors back and forth. That advice can easily be construed as advice that requires expertise, and it really can't be confused with the actual swinging of hammers or the construction means and methods, which would fall under a GL policy. I think we're just going to keep seeing a spike in claims, and I don't think contractors are going to be able to avoid buying coverage."

Finally, Sheehan mentions managed care as another industry with the potential for increased E&O exposures.

"With healthcare distribution changing in our country and public groundswell trying to find ways to cut costs in healthcare, any firm that's in that chain of managing the cost or distribution of healthcare … [has] to be concerned that they are going to be under a regulatory microscope and also be subject to antitrust suits from competitors or regulators."

"I think it's common knowledge now that cyber privacy exposures and risk are a boardroom issue, not just the purview of your chief information officer or IT department"

Matt Sheehan, Worldwide Facilities

WHAT IS FIDELITY INSURANCE?

Fidelity insurance is designed to protect an employer against losses directly resulting from an employee's dishonesty (including theft and embezzlement).

Fidelity insurance

"[Fidelity insurance] provides coverage not only for employee theft, but also for theft committed by a third party, both of which are real risks," says Rachelle Rebick of RT ProExec. "The importance of this kind of protection is increasing because people are always finding new and creative ways to commit the theft or fraud. Technological advances have also helped provide new ways for individuals – or groups of individuals – to commit theft against their employer or another third party."

A key example of an emerging risk in the fidelity space is impersonation fraud, also known as social engineering fraud.

"This type of fraud is a scheme to obtain funds of the company by an individual purporting to be a vendor, client or executive of the company," Rebick explains. "The fraud typically occurs over the phone or in an email. As a result of the significant amount of data about companies and executives on the internet, criminals are easily able to gather information and construct convincing stories, making this type of fraud difficult to prevent, even with the proper controls in place."

Cyber risk

According to Mickey Estey, cyber risk exposure for professional firms is growing rapidly as it relates to data privacy.

"Many classes of professionals have always had a cyber risk exposure. This includes healthcare, attorneys, accountants and other financial professionals," he says. "The thing that has changed is these types of firms are being targeted at a much higher rate and sophistication because the hackers have

> "Technological advances have helped provide new ways for individuals – or groups of individuals – to commit theft against their employer or another third party"
>
> Rachelle Rebick, RT ProExec

recognized that many professionals have what they would consider to be a gold mine of confidential information on individuals that can be sold in the criminal underground."

Estey says there's been an increase in many types of phishing, ransomware and other social engineering attacks against these firms.

"Recently, during tax season, many firms have been hit with W-2 scams, where the hackers send fraudulent emails to try to induce companies to send the W-2s on employees."

Today, it's imperative that cyber risk is on the radars of those charged with running companies. "I think it's common knowledge now that cyber privacy exposures and risk are a boardroom issue, not just the purview of your chief information officer or IT department," Sheehan says. "The SEC has supplied guidelines along those lines, which trickle down through the public and private sector. The risk of cyber and privacy exposures to a company's balance sheet, their reputation and, ultimately, to losing customers and revenue sources is huge."

Sheehan says there's been a disturbing trend among private D&O insurers to add a broad-based cyber network security exclusion to a D&O policy. He says that while the direct costs of a data breach or network security event should be borne by a cyber policy, any subsequent claims by investors, creditors or other stakeholders against management for any failure to manage a company properly – which led to the cyber attack – should be covered under the D&O policy.

"While … it's okay to have that exclusion, we want to limit its scope," he says.

On cyber risk and E&O, Sheehan says there's a perception among professionals that their E&O policy will cover them for any failure to protect confidential information.

"Even if an accountant or an attorney makes the argument that the breach of privacy occurred while providing professional services to that client, there are first-party costs that are expected of that professional firm that don't meet the definition of a 'claim' in an E&O policy," he says. "So those first-party costs would be borne by the organization. Also, the experts that a cyber policy can put into place, and the speed with which they put them into place, can lessen a lot of reputational damage to that firm, as well as hastening a solution to the problem, which the E&O policy will not respond to."

In other words, cyber coverage is crucial.

"A breach or a network shutdown is a huge threat to a company's reputation and, ultimately, their balance sheet," Sheehan says. "When a company's balance sheet and their reputation are harmed, that has a spill-over effect to employee retention, employee hiring and firing – which can hit an employment practices policy – [and] it has spill-over effects for investors, creditors and regulators, which could be the subject of a D&O policy.

"Ultimately," he continues, "it's going to affect the organization's health and risk management practices, which can spill over into any sort of liability exposure that the entity may have. So, the initial problem of a breach or a network interruption can be picked up by a cyber policy, but the follow-on reputational damage and spill-over effects are hard to enumerate."

Client conversations

Given these shifting exposures, brokers need to initiate conversations with their clients to ensure they're able to organize appropriate insurance for those clients' exposures. So what shape should that discussion take?

CYBER INSURANCE FAST FACTS

$2 billion
Amount of total annual cyber premiums in 2015

$20 billion
Amount annual cyber premiums are expected to reach by 2025

$350 to $400 million
Available cyber limits in the marketplace

Source: Willis Marketplace Realities 2016

"Have a casual conversation with your insured about how they actually make money and who they interact with to meet their goals of making money and servicing their clients and, ultimately, providing a good place for their employees to work," Sheehan advises. "Once that conversation happens, you can find out who they actually interact with and what problems can arise."

Estey recommends having an ongoing conversation "as companies change their services, offer new ones or make acquisitions to make sure that the professional coverage is kept up-to-date to contemplate those exposures."

On the cyber and privacy side, he adds: "Evaluate coverage with respect to the professional policy and take the appropriate steps to add broad cyber coverage on the professional policy or add [a] stand-alone cyber policy to address the risk."

Sheehan emphasizes the difference that can be made if those conversations begin early.

"I can't tell you how many times I've had to place a policy in 24 hours because of a contractual requirement – which is fine, and that's what I'm here to do, but if you can start early and tell a clearer story and give multiple underwriters ample time to digest the risk, quote the risk and offer their expertise, without a doubt you're going to come back with a policy that fits the insured's needs better and is likely a more cost-effective option." IB