Insurance Buyers' News

BPJ Insurance

Springfield
PO Box 4207, Springfield, MO 65808
Phone: 800-422-5275
417-887-3550 • Fax: 417-887-3252

Rolla
PO Box 1258, Rolla, MO 65402-1258
Phone: 800-364-2212
573-364-8888 • Fax: 573-341-2257

West Plains
PO Box 964, West Plains, MO 65775
Phone: 800-400-3896
417-256-6162 • Fax: 417-256-6165

River City Insurance
PO Box 127, New Madrid, MO 63869
Phone: 800-899-7392
578-748-5215 • Fax: 573-748-5392

Social Movements | November 2022 | Volume 33 • Number 6

ESG Movement Begins to Impact Insurers

In October, Munich Reinsurance Co., the world's largest reinsurer, announced new stricter policies for investing in and underwriting oil and gas projects, drawing praise from environmental activists.

Munich RE has said on its website that as of April 2023 it would not invest or insure projects involving new oil and gas fields or new midstream oil infrastructure.

As part of its Insure Our Future campaign, Munich Re said its move to restrict what it would underwrite based on concern for the climate was "a significant step and a clear signal to the global insurance market."

Over the past few years insurers have increasingly been tightening their underwriting and restricting their investment policies to exclude polluting industries, though often falling short of activists' demands. But excluding certain industries from their underwriting or investment portfolios is only a part of a wider and more aggressive campaign to change corporate decision-making and transform it based on a new set

of ethical guidelines.

Environmental, Social and Governance (ESG)

It's not only activists who are forcing insurance companies to align their underwriting and investment policies to ideals that overrule decisions based purely on financial returns on investment.

According to consulting firm PwC (formerly Price Waterhouse and Coopers & Lybrand), regulatory de-

continued on next page

This Just In…

In spite of inflation and rising costs, most Americans would rather pay more for insurance coverage than use data-monitoring devices, according to an annual survey from Policygenius.

The survey found that 68% of U.S. consumers said they would not install an app that collects driving behavior or location data for any insurance discount amount, up from 58% in 2021. Of those willing to download a data-collecting app, 67% said they would only do so if their rates were lowered by more than half.

Similarly, 65% of respondents said that no discount is worth installing a smart home device—for example, a doorbell camera, water sensor or smart thermostat—if these devices shared data with their insurance companies, compared to 57% in 2021.

Other survey findings:

- **68% of those surveyed would not install a live dashboard camera for any insurance discount amount. For those who said they would install a dashcam, 74% would only do so if it cut their bill by at least half.**

continued on next page

velopments are forcing insurers to reorient their goals and objectives with environmental, social and governance (ESG) needs in mind.

The climate disclosure requirements of the US Securities and Exchange Commission (SEC), which it released as a proposal in March, is intended to address growing investor demands to understand what companies are doing to manage climate change risks and the transition to a low carbon economy. Although insurers are awaiting more specific guidance from the SEC on some proposal topics, they're facing a move from existing voluntary disclosures of climate-related risks to mandatory requirements that potentially carry increased legal liability.

In addition, the National Association of Insurance Commissioners (NAIC) released an updated climate risk disclosure survey in April. Survey questions align almost entirely with the Task Force on Climate-Related Financial Disclosures (TCFD) framework. This will result in a significant shift towards TCFD-aligned disclosures for US insurers, forcing carriers to think about climate change in multiple facets of their business and confront how they address it.

Insurers Need a Focused ESG Strategy, says Consultant

As a result, a formal and clearly defined ESG strategy is no longer optional, according to PwC. Not only do key stakeholders want explanations of how insurers are addressing the issue, says PwC, according to its survey of leading global insurers, they're also formally mandating them.

- 25% of global insurers told us that "understanding ESG-related regulations and guidelines" is the main challenge in pushing forward their ESG agenda, followed by "understanding how best to take action on ESG" (17%) and "matching ESG initiatives with customer needs" (15%).
- 49% of insurance CEOs say their company does not have the ability to measure their greenhouse gas (GHG) emissions today, despite the SEC's proposal for new climate disclosure requirements. 85% of global insurers believe ESG will impact all functions of their business. They identified investments as the single largest area of impact (91% respondents), followed by risk and internal audit (90%) and underwriting (88%).
- Global insurers tell us that the main driver of their ESG pursuit is "to minimize the impact from climate change" (26%), "to gain a better reputation as a firm" (11%) and "to minimize risk" (11%).

However, PwC says that of the "three pillars of ESG," as it defines them, only 35% of global insurers are "significantly focused" on all three of them.

Yes, there are three and environment is only one:

Environment pillar: climate

- Mitigate climate change risks (62%).
- Meet customer expectations (61%).
- Drive product/service innovation (54%).
- Satisfy investor demands (51%).

Social pillar: building trust

- 69% of global insurance CEOs tell us they are extremely or very concerned with the impact of social inequality on their ability to attract and retain key skills.
- 49% of global insurance CEOs tell us they are extremely or very concerned with the impact of social inequality on their ability to sell products and services.

This Just In

- **77% of respondents would not install a smart doorbell camera that shares facial recognition data with third parties for any home or renters insurance discount amount, an increase from 67% in 2021. Of the 23% willing to install smart doorbell cameras, 68% of people would only do so if the cost of their home insurance was cut at least in half.**
- **Of the 35% of homeowners and renters willing to install smart home devices for insurance discounts, 69% would only do it for a discount of half their bill or more.**

"Although policyholders can often get lower insurance rates by agreeing to share personal information about their daily activities with their insurance providers, it's clear consumers are overwhelmingly uncomfortable allowing data-sharing devices into their everyday lives," said Andrew Hurst of Policygenius.

- Increasing shareholder value is among the top priorities in all regions, while creating a fairer society is a primary driver exclusively in Europe.

Governance pillar: incentives

ESG calls for responsible organizational actions and behaviors, including transparency, and well-understood and clearly communicated business ethics, as well as the recognition that diverse viewpoints lead to more informed decisions. PwC says carriers still have far to go in this area.

Less than half of FTSE 100 companies have tied executive pay to ESG measures and progress has been even slower further down the chain of command. This represents a prime opportunity for carriers to embed ESG objectives into the entire organization and increase employee commitment to the according to PwC.

90% of Risk Managers at Least Moderately Concerned about Cyber Attacks

A recent survey of risk managers—those charged with identifying, evaluating, and selecting the best techniques to mitigate risk—by Nationwide Insurance revealed that cybersecurity takes up a substantial portion of their budgets. 68% expect these budgets will continue to grow in the coming years.

Nationwide's previous studies have revealed that consumers as well as small to mid-sized businesses have begun to take cyber threats very seriously," said Tim Nunziata, Vice President of Cyber Risk for Nationwide Excess and Surplus/Specialty. "Large businesses have always been a target and that's why many already have teams in place to protect them. As the threats become more frequent and sophisticated, risk managers know they must remain vigilant."

War with Ukraine Increased Cyber Risks

Respondents believe there is a greater risk of their company experiencing a cyberattack since the beginning of the war in Ukraine (57%). 90% say they are concerned about their company falling victim to a cyberattack. But they are preparing, 91% have an incident response plan in the event of a cyberattack.

68% of those who took part in Nationwide's survey report their company has been the victim of an attack in the last three years, including almost 1 in 4 (24%) in the past year. 88% say that they've experienced an attack at some point in their company's history.

continued on next page

Attacks Are Costly, and Recovery Takes Time

Of those who experienced an attack nearly 7 in 10 (68%) report their business operations were impacted and three-quarters (75%) reported a significant or moderate financial impact.

71% said recovery from the attack took longer than one month, and more than a third (35%) reported the process taking longer than four months.

They view data breaches (24%), ransomware (13%) and business interruption (11%) as the top cybersecurity threats.

Deepfakes on the Horizon

Risk managers are on the lookout for common attacks but there's a new threat to keep an eye on. The cyberattack of the future? Deepfakes — a type of artificial intelligence used to create convincing images, including audio and video hoaxes, often with malicious intent. Despite an increase in companies falling prey to deepfake attacks and even warnings from the FBI, it's not high on the list of concerns for risk managers. Only 6% of those surveyed say social engineering, impersonation, or other tactics to manipulate employees is their biggest concern.

Cyber Insurance is Key

Companies are turning to insurance experts for help. 83% report they are renewing their current cyber policy. 94% of those who did renew that policy said their broker or agent played an important role during the renewal process. Half (53%) of risk managers report their coverage has changed in the past two years, with most reporting that they've increased their coverage.

"Agents and brokers can help clarify the threat landscape, including what is out there and what cyber trends they are seeing," said Nunziata. "Where they really provide value is making sure a business has the coverage they need to protect and mitigate issues."

5 Tips for Getting the Best Cyber Coverage

Not all cyber policies are the same and there are certain features and enhancements you need to be aware of. Here are five of them:

1. Obtain Retroactive Coverage

Many cyber policies are claims-made, meaning they will only cover incidents that occurred during the policy period. Let's say your cyber policy has an inception date of January 1, 2022, and several days later you discover that three months previously you started having cyber breaches. The incidents that occurred prior to January 1, 2022, will not be covered under a claims--made policy. The solution is to buy coverage extending back 2, 4, 6 or even 10 years, unless you can simply buy an occurrence form.

2. Beware of Panel and Consent Provisions

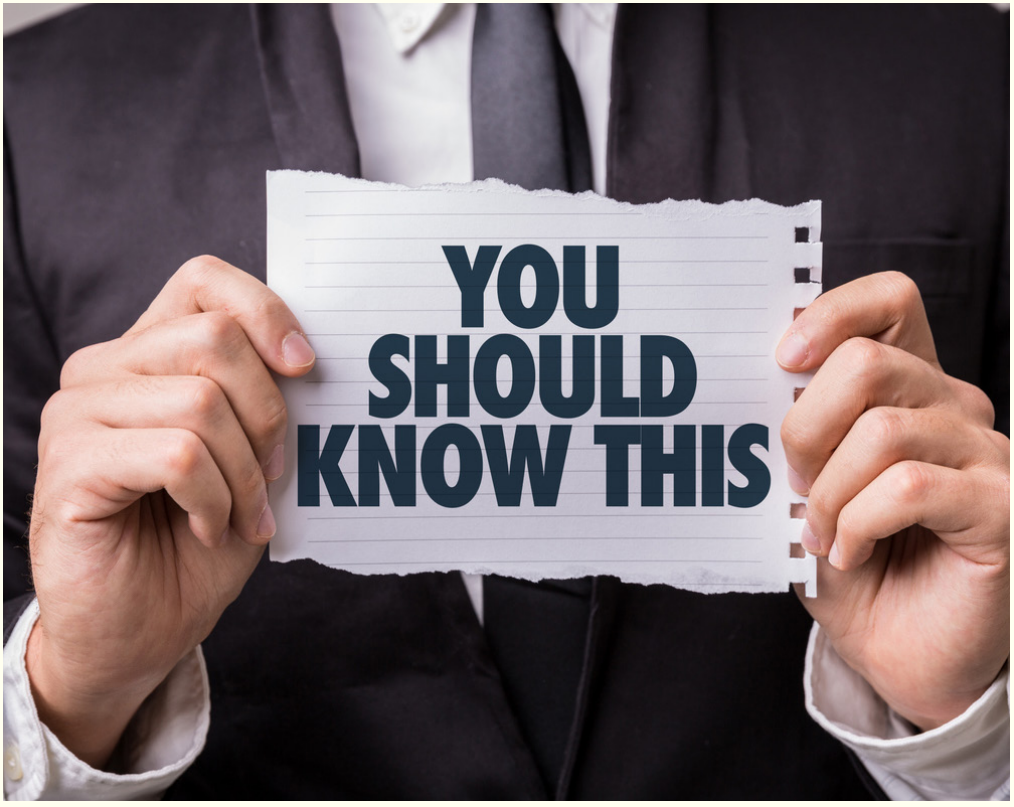
Many cyber policies require that the investigators, consultants or attorneys used to respond to a cyber claim must be drawn from a preapproved list. If you have consultants you would like to work with in the event you have to file a claim, ask that they be added to the list.

As James Bobotek, a partner at Pillsbury Winthrop Shaw Pittman in McClean, Virginia, points out, "Cyber policies also often contain provisions stating that the policyholder must obtain the insurer's consent before incurring any expenses to notify customers of a data breach, conduct forensic investigations, or defend against third-party claims. Insurers sometimes invoke these provisions to deny coverage when emergency costs have been incurred without the insurer's consent, even if the costs are entirely reasonable and necessary. If prior-consent provisions are included in the policy you are considering and cannot be removed, you should, at a minimum, change them to provide that the insurer's consent 'shall not be unreasonably withheld."

3. Pay Attention to How Defense Costs Are Allocated

Sometimes lawsuits involve claims covered by a cyber policy as well as claims that are not. What portion of the policyholder's defense costs will be paid from the cyber policy?

continued on next page



As James Bobotek points out, some policies say that the insurer will pay all defense costs if the lawsuit alleges any claim that is potentially covered. Others stipulate that the insurer will only pay costs that it unilaterally believes to be covered unless or until a different allocation is negotiated, arbitrated, or determined by a court.

These issues are less likely to arise under a "duty to defend" policy, where the insurer must assume the defense of any third-party claims. This type of policy typically covers all defense costs as long as any of the claims are potentially covered. However, under a "duty to reimburse" policy, where the insurer agrees to reimburse the policyholder for its defense costs or pay them on its behalf, allocation is more likely to be disputed.

Be sure you understand the allocation method contained in the policy you are considering. Try to negotiate one that is favorable to you.

4. Be Sure You Have Coverage for Vendor Acts and Omissions

At least a part of an organization's data may be outsourced to third parties. It's crucial that your policy cover you for breaches they may cause. Most but not all cyber policies cover "vicarious liability" for acts and omissions of vendors, consultants and sub-contractors. Be sure your policy language is not ambiguous about this.

That said, you should also require that vendors and others in whose care you place your data have adequate cyber insurance themselves and name you as an additional insured. Get a certificate of insurance.

Also, your policy should state that when their insurance applies, your insurance should only apply after the vendor's insurance coverage has been exhausted.

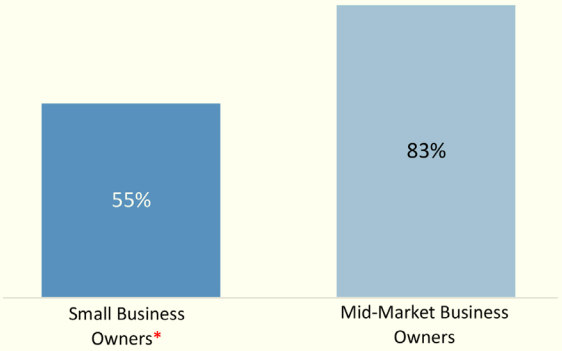
5. Get a Partial Subrogation Waiver

When you have a loss, your insurer is typically "subrogated" to any claims you may have against third parties. This allows your insurer to recover funds they paid to you by going after your vendors if they were culpable for those losses. To fortify your insurer's rights in that respect, your policy may say that you cannot do anything to impair your insurer's right to subrogation. The problem is that many contracts with data managers state that their liability to you is limited. That can put you in breach of your insurance contract. The way to fix this problem is to obtain a partial waiver of subrogation for your cyber policy. This will provide that the insurer will not assert that its right of subrogation has been impaired by any contracts you entered with vendors prior to a loss.

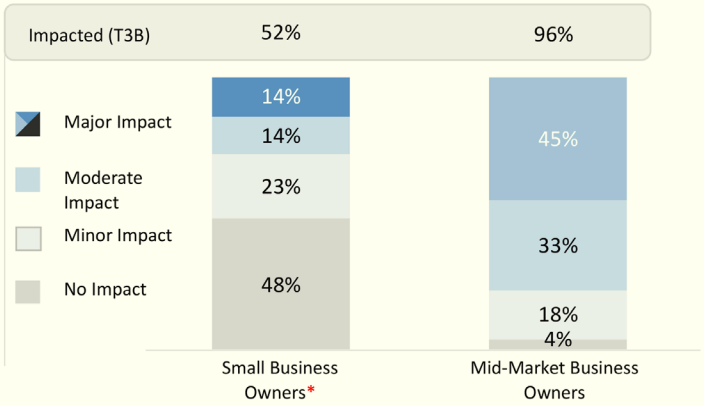
Mid-Market Business Owners overwhelmingly agree cyberattacks have jeopardized their business and negatively impacted customer trust

In contrast, just over half of Small Business Owners said the same.

Cyberattack Impacted or Jeopardized Business Finances
(Shown % Select 'Yes')



Cyberattack Negatively Impacted Customer Trust in Business
(Shown % Select)



*Low sample, directional only

Q9a. Did the cyberattack impact or jeopardize your business / your personal finances? // Q10. Which of the following best describes your situation when the cyberattack occurred? Base: Small Business Owners (n=56), Mid-Market Business Owners (n=187).*

Insurance Buyers' News