cafii acifa
The Canadian Association of Financial Institutions in Insurance | L'association canadienne des institutions financières en assurance

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

CAFII ALERTS WEEKLY DIGEST: May 6-10, 2024

May 10, 2024

The CAFII Alerts Weekly Digest is intended to provide a curated compendium of news on insurance, regulatory, and industry/business/societal topics of relevance to CAFII Members – drawn from domestic and international industry trade press and mainstream media – to aid in Members' awareness of recently published media content in those areas.

TABLE OF CONTENTS

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

GOVERNMENT/LEGAL/REGULATORY/ BUSINESS DEVELOPMENTS

Alberta Insurance Council's New CEO Set To Drive Change

Find Out Her Key Priorities…

By Nicole Panteloucos, Insurance Business, May 06, 2024

https://www.insurancebusinessmag.com/ca/news/breaking-news/alberta-insurance-councils-new-ceo-set-to-drive-change-488018.aspx?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240506&_hsenc=p2ANqtz-8xePiRvYWMJe4jNpkG-Znu-cDIx6mlh1PD1wsbvDe5lTEZcSJN5e95NROxlxnkqBUZSyyRXm0B2e9jvI70p3aARkL-1w&_hsmi=305814926&utm_content=&utm_source=

In a recent announcement, the Alberta Insurance Council (AIC) revealed Amina Deiab (pictured) as its newly appointed chief executive officer, formally stepping into the role on April 22.

Despite being just two weeks into her tenure, Deiab has already started laying out her ambitious plans to lead the AIC into a new era of success.

Building Relationships

Speaking on her new role, Deiab said she plans to focus on building collaborative relationships with the council's stakeholders.

"Over time, regulatory agencies can start to have an inward turning focus. And it's important for regulators to keep pace with changes in the industry," she said. "A defining measure of success, certainly, for me, and for the organization, is working very collaboratively with our stakeholders."

While maintaining strong partner relationships is imperative, Deiab also stressed the significance of establishing a positive culture within her own team.

"We want to build an environment where our staff are excited to come into work every day. There is no organization without our people, who are the backbone of the organization. It's very much about taking care of our people. And of course, they take care of our business," said Deiab.

With AIC offices in Calgary and Edmonton, Deiab hopes to bring the two teams together whenever possible, through celebrating staff success and organizing team-building initiatives.

Modernizing Practices

Deiab has also set her sights on refreshing the council's operations.

"I think an opportunity for the AIC and for the insurance regulatory sector is modernization, it's taking business practices and applying them into the regulatory environment," she said.

"That includes thinking about how we expand our education, both for consumers as well as for licensees."

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Part of the CEO's plan for consumer education involves digital outreach.

For the first time in AIC's history, Deiab revealed the council will launch a communications campaign focused on consumer protection. The campaign will include a social media rollout set to complement its newly refreshed website, which is scheduled to launch in July.

"It's a beautiful website. I'm really excited about it. It makes it easier for both our licensees and consumers to find information in a timely way," she said.

Risk-Based Regulation

Seeking to transition the AIC into a more outcome- and risk-based regulatory body, Deiab emphasized the pivotal role of data analytics in her long-term strategy.

"As a regulator, we have a lot of data. It's about being able to leverage that data over time to form the basis of risk-based regulation," she said. "What that means is looking across all our regulatory activities, and asking the question, do we have the right resources, at the right time, in the right place?"

Acknowledging the AIC's 30-year legacy, Deiab noted that shifting towards data automation will be a significant change and she remains determined to propel the council into its next phase of development.

"Change management takes time and it's not just about the data and the analytics and our systems, it's about how can we work together in a different way," she said.

FSRA Chief Tapped For Ontario Energy Board

Proposed Appointment Still Needs To Be Confirmed By Legislative Committee

By James Langton, Investment Executive, May 03, 2024

https://www.investmentexecutive.com/news/from-the-regulators/fsra-chief-tapped-for-ontario-energy-board/?utm_source=newsletter&utm_medium=nl&utm_content=investmentexecutive&utm_campaign=INT-EN-morning&hash=f9f4f6eaaf33f1b05c846d7c2a532f58

The head of the Financial Services Regulatory Authority of Ontario (FSRA), CEO Mark White, has been tapped to take over as chair of the Ontario Energy Board.

FSRA said it will announce the details of its succession plan for White if the appointment is approved.

White's nomination must still be reviewed by the Standing Committee on Government Agencies before his appointment can be confirmed.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

"Until the appointment is confirmed, it will be business as usual at FSRA," said FSRA chairperson Joanne De Laurentiis in a release.

White has served as FSRA's first CEO since May 2018. He presided over the implementation of Ontario's title protection framework, which established a minimum standard of proficiency for financial advisors and planners for the first time. However, the framework has come under criticism for its multiple-credential approach and, for advisors, its product focus.

Before joining FSRA, White was senior vice-president & head enterprise risk at the Bank of Montreal (BMO). He joined the bank from the Office of the Superintendent of Financial Institutions, and previously worked at RBC Capital Markets and Ernst & Young LLP, among other roles.

OTHER CAFII MEMBER-RELEVANT NEWS

No Room For Weak Links With Compliance

Gallagher Bassett Has The Knowledge And Capacity To Help Insurers Get Regulatory Compliance Right

By Bennett Richardson, Insurance Business, May 07, 2024

https://www.insurancebusinessmag.com/au/news/cyber/no-room-for-weak-links-with-compliance-486959.aspx?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240507&_hsenc=p2ANqtz--q4bZjBnOwQ-Td5jvC2IHJK1WwO1N3_NIK-fIIe9Q64_aEBOPRJEUve7CjwqludloDMIaOoxk8aUX_BW43_8OXRgYlqw&_hsmi=306003556&utm_content=&utm_source=

This article was produced in partnership with Gallagher Bassett.

Keeping up with compliance requirements is becoming tougher for insurers to handle on their own – and insurers know it.

A new Gallagher Bassett survey, released as part of The Carrier Perspective: 2024 Claims Insights report, reveals issues such as data privacy, staying abreast of regulation changes, and cybersecurity as some of the leading concerns for insurers worldwide and in Australia.

Insurers with stretched resources in a tough market know they need to act, but many have more questions than answers about how to handle the increasing burden.

"There are certainly important questions that need to be addressed. Do carriers have a comprehensive strategy or plan in place to address a cyber event? Are their vendors lined up to act promptly as needed? How do carriers ensure their data is encrypted, and do they have measures in place to duplicate data if necessary?", said Archana Acharya, Chief General Counsel at Gallagher Bassett Australia.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Acharya's answer is simple – a problem shared is a problem halved.

"Using outside specialists emerges as the foremost strategy, with many carriers seeking advice from claims management providers, legal advisors, and compliance consultants. The old adage that 'you are only as strong as your weakest link' requires insurers to be just as demanding of their supply chain, which is often vested with personal information, as they are of their own internal standards", she said.

Compliance Tasks Likely To Increase Significantly

Regulatory compliance is an area that is only going to increase in complexity, making the task of getting it right more difficult for insurers that may have managed until now.

The growth of regulations globally around data matters is a key risk for tech firms with business offshore, for example. Most tech firms have reporting obligations in multiple regimes and the rules in those regimes are constantly on the move.

Several states in the US passed or amended privacy regulations in the last few years. Updates to privacy laws related to the General Data Protection Regulation (GDPR) in the EU or extension of regulations from the California Consumer Privacy Act with the California Privacy Rights Act, which took effect in 2023, are some of the latest rules that tech firms need to be across in terms of their professional indemnity obligations. In 2024, more regulatory change is also expected in the EU, the UK, Singapore, Australia, and Japan.

This means that compliance resources at many insurers may become stretched to breaking point. But Gallagher Bassett is well placed to fill the role of compliance expert and not only relieve the burden, but also provide a better service to customers.

Partnering With Experts Can Lift Profits And Competitiveness

"By leveraging specialist knowledge, insurers can navigate the complexities of customer-focused regulations. This approach facilitates compliance and underscores their commitment to a forward-thinking strategy", said Acharya.

Gallagher Bassett research shows that 43% of global and 53% of Australian insurers plan to hire compliance consultants or claims and risk management experts to enhance and maintain compliance measures.

"Moreover, a strong trend is emerging around partnering with claims management providers, with 30% of global and 43% of Australian insurers exploring this avenue to fortify their compliance strategies", said Joe Powell, Senior Vice President of Analytics at Gallagher Bassett.

"Collaborating with a claims and risk management provider can help streamline claims processes and foster a proactive approach to ongoing adherence to changing customer-focused regulations", said Acharya.

Outsourcing compliance allows insurers more time to deal with other key aspects of the business, including customer care and seeking out new sources of revenue. These partnerships empower leaders to increase profitability, enhance brand reputation, and outpace competitors.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

The Compliance Issues That Most Concern Insurers

Both globally and in the UK, the main compliance and regulatory challenge that insurers anticipate for 2024 is data privacy and security compliance. According to the Gallagher Bassett survey, this issue was identified as the primary concern by 75% of global and 83% of Australian insurers.

For most anticipated compliance and regulatory challenges, Australian insurers were more concerned than their global peers, perhaps underscoring the increased level of regulation in the region and the growing burden it poses.

Staying abreast of regulatory change is more of a concern for Australian insurers than globally, as is cybersecurity and data breach regulations, adoption of consumer protection laws, and navigating international regulations.

A significant focal point for insurers worldwide is cybersecurity and data breach regulations: Gallagher Bassett data shows that 63% of insurers globally and 65% in Australia anticipate this evolving challenge.

Cyber Issues Increasing In Volume And Severity

Cybersecurity and data security threats are unlikely to abate any time soon. The 2024 Thales Data Threat Report, based on a survey of nearly 3000 IT and security professionals in 18 countries across 37 industries, found that 93% of IT professionals believe security threats are increasing in volume or severity, a significant rise from 47% last year.

Thales found that there was a very clear correlation between compliance and data security. Of those organisations that had failed a compliance audit in the past twelve months, 31% had experienced a breach that very same year. This compares to just 3% of those who had passed compliance audits.

Regulatory reporting and documentation management is another key concern, with 48% of insurers in Australia expecting this to be challenging versus only 43% globally. This is pushing insurers to re-evaluate their reporting mechanisms.

Clearly, not keeping up with compliance in 2024 is not an option. In a fast changing regulatory and threat environment, there is inevitably a lag in understanding what systems, applications, and data are at risk, making it vital to line up proper and robust plans of action.

“By embracing robust cybersecurity measures, reinforcing consumer protection laws, and optimising reporting processes, insurers can ensure adherence to regulatory standards and position themselves to adjust and grow in an era of unprecedented change”, said Acharya.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

ESG Discussions With Clients Lacking, Research Suggests

Secret Shopper Exercise Highlights The Need To Align Client Goals With Appropriate Investments

By Noushin Ziafati, Investment Executive, May 06, 2024

https://www.investmentexecutive.com/news/research-and-markets/only-20-of-advisors-bring-up-esg-investments-unprompted-report/?utm_source=newsletter&utm_medium=nl&utm_content=investmentexecutive&utm_campaign=INT-EN-morning&hash=f9f4f6eaaf33f1b05c846d7c2a532f58

A secret shopper campaign conducted by a provider of ESG training suggests financial advisors can improve the service they provide to clients who are interested in sustainability.

Montreal-based ED4S Academy conducted the research in the first two months of 2024. Posing as customers, ED4S associates spoke to 40 Canadian advisors at 35 firms, including big banks, credit unions, insurance companies and smaller asset management firms.

The secret shoppers had a background in sustainable finance, and the research results were released in a report on Monday.

The research found that 20% of the advisors (eight advisors) brought up ESG or sustainability considerations to the secret shoppers without any prompts. Once the secret shoppers showed interest in ESG issues, this metric increased to about 63%.

When the secret shoppers told the advisors that their primary concern was climate change action, an "encouraging" 25% of advisors were able to discuss client goals and investment approaches to address climate change, the report said. However, other ESG issues weren't discussed, such as water, land use and pollution.

The report said that about half of the advisors (45%) demonstrated a "sufficient" understanding of ESG investment approaches, and another 25% were "somewhat" knowledgeable.

An advisor's knowledge was deemed "sufficient" if they demonstrated a basic understanding of sustainable investment issues or themes such as climate change.

"We did not expect encyclopedic knowledge of sustainability issues from advisors, but rather the ability to understand a client's ESG priorities and propose appropriate investment solutions," the report said.

As far as available products, while most advisors offered some ESG or sustainable investments, the secret shoppers considered those products a good fit 17% of the time, and "somewhat of a good fit" 39% of the time.

The research also found that about 63% of advisors (or about 25 advisors) discussed the performance of sustainable investments. However, about one-third (35%) of advisors said sustainable fund performance was the same as that of other investments.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

"The real answer to this question depends on the time frame, and how sustainable investment products are defined," the report said.

In more than half of client discussions (55%), advisors did not discuss the fees of sustainable investments, the report said.

The report said that given the overall findings, sustainable investments seem to be "a secondary consideration if not a niche asset class" among the advisors studied.

Responsible investments accounted for 49% of assets under management in Canada in 2022, up from 47% in 2021, based on the 2023 Canadian Responsible Investment Trends Report. That report attributed the increase to a global movement to enhance sustainability reporting.

The ED4S report did not mention such reporting. However, it suggested that firms ensure they have the sustainable investment products that investors desire.

It concluded that as sustainable investment products become more common and well-defined, "investors and advisors need to have the conversations necessary to align investment objectives with the products available."

What Constitutes An AI Risk – And How Should The C-Suite Manage It?

"Potential Can Be Harnessed" With The Right Moves

By Kenneth Araullo, Insurance Business, May 06, 2024

https://www.insurancebusinessmag.com/ca/risk-management/news/what-constitutes-an-ai-risk--and-how-should-the-csuite-manage-it-488063.aspx?hsmemberId=83982452&tu=&utm_campaign=&utm_medium=20240507&_hsenc=p2ANqtz--wvYj3xZAEszhEuV3bLXrH2kARzHAvKOZDJHZJP-zJSB-tKyARYCHHPiRTuVBZPY_VV7lFs_SvOpg9-qUvFWSGN05fxg&_hsmi=306003556&utm_content=&utm_source=

As artificial intelligence (AI) becomes increasingly integrated into corporate operations, it introduces a complex array of risks that require meticulous management. These risks range from potential regulatory infractions and cybersecurity vulnerabilities to ethical dilemmas and privacy concerns.

Given the significant consequences of mismanaging AI, it is essential for directors and officers to establish comprehensive risk management strategies to mitigate these threats effectively.

Edward Vaughan (pictured above), a management liability associate at Lockton, has emphasized the intricate challenges and responsibilities associated with integrating AI into business operations, particularly noting the potential liabilities for directors and officers.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

"To be prepared for the potential regulatory scrutiny or claims activity that comes with the introduction of a new technology, it is imperative that boards carefully consider the introduction of AI, and ensure sufficient risk mitigation measures are in place," Vaughan said.

AI significantly enhances productivity, streamlines operations, and fosters innovation across various sectors. However, Vaughan notes that these advantages are accompanied by substantial risks such as potential harm to customers, financial losses, and increased regulatory scrutiny.

"Companies' disclosure of their AI usage is another potential source of exposure. Amid surging investor interest in AI, companies and their boards may be tempted to overstate the extent of their AI capabilities and investments. This practice, known as 'AI washing', recently led one plaintiff to file a securities class-action lawsuit in the US against an AI-enabled software platform company, arguing that investors had been misled," he said.

Furthermore, the regulatory landscape is evolving, as seen with legislation like the EU AI Act, which demands greater transparency in how companies deploy AI.

"Just as disclosures may overstate AI capabilities, companies may also understate their exposure to AI-related disruption or fail to disclose that their competitors are adopting AI tools more rapidly and effectively. Cybersecurity risks or flawed algorithms leading to reputational harm, competitive harm or legal liability are all potential consequences of poorly implemented AI," Vaughan said.

Who Is Responsible For These Risks?

For directors and officers, these evolving challenges underscore the importance of overseeing AI integration and understanding the risks involved. Responsibilities extend across various domains, including ensuring legal and regulatory compliance to prevent AI from causing competitive or reputational harm.

"Allegations of poor AI governance procedures or claims for AI technology failure as well as misrepresentation may be alleged against directors and officers in the form of a breach of the directors' duties. Such claims could damage a company's reputation and result in a D&O class action," he said.

Additionally, given the vulnerabilities associated with digital technologies, protecting AI systems from cyber threats and ensuring data privacy are critical concerns. Vaughan notes that transparent communication with investors about AI's role and impact is also crucial to managing expectations and avoiding misrepresentations that could lead to legal challenges.

Directors might face negligence claims from AI-related failures, such as discrimination or privacy breaches, leading to substantial legal and financial repercussions. Misrepresentation claims could also arise if AI-generated reports or disclosures contain inaccuracies.

Furthermore, directors must ensure that appropriate insurance coverage is in place to address potential losses induced by AI, as highlighted by insurers like Allianz Commercial, who have specifically warned about AI's implications for cybersecurity, regulatory risks, and misinformation management.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Risk Management For AI-Related Risks

To effectively manage these risks, Vaughan suggests that boards implement comprehensive decision-making protocols for evaluating and adopting new technologies.

"Boards, in consultation with in-house and outside counsel, may consider setting up an AI ethics committee to consult on the implementation and management of AI tools. This committee may also be able to help monitor emerging policies and legislation in respect of AI. If a business doesn't have the internal expertise to develop, use, and maintain AI, this may be actioned via a third party," he said.

Ensuring employees are well-trained and equipped to manage AI tools responsibly is crucial for maintaining operational integrity. Establishing an AI ethics committee can offer valuable guidance on the ethical use of AI, monitor legislative developments, and address concerns related to AI bias and intellectual property.

In conclusion, Vaughan said that while AI offers significant opportunities for growth and innovation, it also necessitates a diligent approach to governance and risk management.

"As AI continues to evolve, it is essential for companies and their boards of directors to have a strong grasp of the risks attached to this technology. With the appropriate action taken, AI's exciting potential can be harnessed, and risk can be minimized," Vaughan said.

How Cybersecurity And Insurance Can Reduce Risk And Enhance Security

By Stu Sjouwerman, Digital Insurance, April 23, 2024

https://www.dig-in.com/opinion/how-cybersecurity-and-insurance-can-reduce-risk?utm_campaign=NL_DIG_Morning_Briefing_04242024&position=2&utm_source=newsletter&utm_medium=email&campaignname=NL_DIG_Morning_Briefing_04242024&oly_enc_id=1794I9343067F0V

Data breaches, ransomware attacks and social engineering scams are becoming an everyday affair. Cyber incidents are also becoming more financially damaging with each passing year, making it harder for organizations to recover. The average cost of a data breach (at $4.45 million) has risen by 15% over the past three years, while the median recovery cost of a ransomware attack stands at about $1.82 million, excluding the cost of the ransom.

To counterbalance these risks proactively and to reduce financial exposure, more organizations are opting for cyber insurance to partially cover losses from a range of information risks. That being, insurance should not be a substitute for cybersecurity. Here are five reasons why:

1. Cyber insurance will only compensate a portion of financial losses
When an attack or breach happens, there is a lot more at stake than just money. A cyberattack can result in loss of intellectual property, loss of customer trust and confidence, loss of reputation, loss of competitive edge and productivity. It can be difficult to quantify these losses and insurance claims will not recoup all that is lost.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

2. Paying the ransom does not always guarantee outcomes
Insurance money might help pay the ransom, but paying the ransom does not always guarantee that threat actors will release the encryption key or return the hijacked data. Most victims (92%) fail to receive their data after paying the ransom. There is also no guarantee that threat actors will not repeat the offense. On the contrary, paying the ransom only encourages malign actors to perpetuate their attacks.

3. Cyber insurance policies too have exclusions
As cyberattacks increase, insurance claims are also rising, introducing more risk to insurers. To offset these losses, insurers have begun tightening policy guidelines and introducing exclusions that allow them to reject or deny claims under specific conditions. For example, 21% of cyber policy holders have a clear ransomware exclusion. While a standard clause among insurers, the language around war exclusions is murky at best. Defining whether a hacktivist is operating solo or in concert with a nation-state is a big unknown; geopolitical adversaries typically deny affiliation with ransomware gangs.

4. New disclosure rules raises insurance risk
The Security and Exchange Commission (SEC) has mandated that publicly traded companies report cyber incidents within four days of determining whether an incident will have a material or substantial impact on shareholders. These new rules enable insurers to scrutinize their client's cybersecurity and governance practices more closely. It is also worth noting that the U.S. government is already mulling over an outright ban on ransomware payments.

5. Cyber insurance is not a replacement for security obligations
Every business has an obligation to protect its information assets as well as its customers, employees, business partners and their data against cyberattacks and data breaches. Simply transferring this risk to a third-party insurance provider does not absolve them of these responsibilities or obligations.

What Can Organizations Do To Reduce Their Risk Exposure?

Cyber insurance is certainly beneficial for businesses; however, it must only be seen as a contingent strategy to cover sudden or unexpected risks. Cyberattacks are more inevitable than they are a probability. It is critical that organizations focus on real mitigations involving technology, people, policies and processes, and not depend solely on insurance policies. Here are some recommended best practices:

1. Have a robust cybersecurity program in place: Deploy multi-layered cybersecurity defenses (multi-factor authentication, firewalls, email security, web security, et. al.) along with clear cybersecurity policies and processes. Organizations seeking insurance coverage may need to undergo security audits to verify they meet minimum security standards.

2. Train employees well: 74% of cyberattacks and breaches are caused by human error. Organizations can significantly reduce exposure to security incidents by providing employees with in-person training and regular phishing and social engineering simulation exercises to help identify and report these malign attacks. Some cyber insurance providers offer security tabletop exercises, training videos and breach response scenarios for insureds. Take advantage of those materials, services and content to train your people.

*3. Adhere strictly to compliance and regulatory mandates:*Be sure to implement industry-leading guidelines, frameworks and compliance standards to ensure that all required and recommended protections and practices are followed.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

Insurers are known to deny claims if they discover that a company has misstated its adherence to certain privacy laws or regulations.

Final Thoughts

A strong partnership between cybersecurity and cyber insurance can foster a robust security culture and reduce risks. Organizations understand that having insurance alone does not mean they can forego implementing necessary security measures. Relying solely on insurance coverage undermines both the insurance carrier and policyholder. Both stakeholders are genuinely more satisfied when strong security protocols are in place, as this lowers the overall risk profile.

When cybersecurity and insurance work in tandem, organizations can build a more resilient security culture. Both policyholder and carrier benefit since the coordination of efforts can narrow the likelihood of filing claims. Cybersecurity plays a pivotal role in mitigating cyber threats. It involves strong access controls, continuous cybersecurity training and simulated phishing exercises, incident response plans, regular risk assessments, and monitoring systems for any signs of compromise. Proactive cybersecurity measures can greatly reduce the likelihood and impact of cyber incidents and potentially lower premiums.

Cyber insurance providers can support the security mission by offering risk assessments, security consulting, and resources to help organizations improve their security posture. Acting as a safety net to ensure organizations have the capacity to bounce back from incidents, cyber insurance provides coverage for costs associated with incident response, recovery, legal fees, regulatory fines, and potential lawsuits.

By collaborating closely, cybersecurity professionals and insurance providers can share insights, best practices, and trends in cyber threats, leading to a more stable and secure environment for all parties involved.

---

5 Trends Shaping Insurance in 2024

Technologies such as AI are reducing costs for underwriters, which will translate to more competitive customer rates.

By Nicos Vekiarides, Insurance Thought Leadership, March 25, 2024

https://www.insurancethoughtleadership.com/ai-machine-learning/5-trends-shaping-insurance-2024

Policyholders may look back on 2023 and remember the trend of premium increases. However, new technologies such as artificial intelligence (AI) are reducing costs for underwriters, which will translate to more competitive customer rates.

You can expect the remainder of 2024 to bring continued technological improvements powered by AI. Policyholders can insure more assets in less time, while carriers continue to reap the cost benefits of greater efficiencies. Of course, when it comes to emerging tech like AI, it's not all good news. New technologies can be used to cheat the system as well as benefit underwriters and policyholders.

200-411 Richmond Street E, Toronto, ON M5A 3S5
(416) 494-9224 (416) 967-6320
info@cafii.com www.cafii.com

When we take a closer look at AI applications in the insurance industry, here are five trends we anticipate seeing in the months ahead:

Insurance On-Demand

Are you renting out your vacation home, trailer or snowmobile? Consumers can monetize their assets through rental companies and online brokers. If you plan to rent your assets, particularly for short-term use, insurance is necessary and can't be left to the renter's discretion

You must be sure that your assets are adequately covered and that you are protected from personal liability. Thankfully, with on-demand policies, getting the necessary coverage becomes simple, whether you are a renter who requires a policy or an owner looking to guard against liability. With the help of AI risk assessment, your policy is ready in minutes and can be customized to your specific needs.

Embedded Insurance Everywhere

Sure, you may know how to add insurance for your purchases or services, but why not sign up at the point of sale and make it all a simple transaction? After all, who wants to wait and go through yet another transaction to add insurance? This process isn't a new strategy. For example, travel insurance is often offered with a plane ticket.

What's new is that embedded insurance is being extended to other purchases, whether it's concert tickets, a new e-bike, ride-sharing or online banking. Embedded insurance reduces risk for consumers and avoids their having to shop for coverage. Just sign on the dotted line to include insurance with your purchase, and, who knows, the merchants may give you a special deal you can't find elsewhere. Embedded insurance presents an opportunity for insurers to capture new customers before they have a chance to shop for coverage.

UPCOMING CAFII-RELEVANT WEBINARS & EVENTS; AND RELATED EDUCATION CONTENT

THIA's 2024 Annual Conference

Date: May 22-24, 2024
Location: Quebec City, Canada

THIA's conference is the highlight of the Canadian travel insurance year and for the first time we are hosting this special event on Canadian soil. We expect to welcome many returning attendees and, by holding our premier event in beautiful Quebec City, we hope to meet many first-time attendees as well.

As always, you won't want to miss:

- Engaging insights from industry experts
- Networking opportunities with peers and prospects from across the globe

A chance to participate in scheduled professional and leisure activities

Register Here - *'Early Bird' registration for THIA and UStiA members is $1,025 CAD until March 31, 2024.*