A PRIVATE MATTER

RIFE WITH SENSITIVE INFORMATION, WORKERS' COMPENSATION DATA IS AN EASY TARGET FOR HACKERS, AND WHILE CYBER INSURANCE HASN'T BEEN WIDELY ADOPTED, STEPS HAVE BEEN TAKEN TO SHORE UP SYSTEMS SECURITY AND PROTECT CLAIMANT PRIVACY

Administering self-insured workers' compensation programs is so fraught with complexity and confusion that data privacy could be compromised by inattentive administrators along the way to securing insurance coverage and mitigating claims.

The work comp area is a treasure trove of personal identifiable information (PII) such as name, date of birth and Social Security number, as well as personal health information (PHI). But there are systemic problems with attempts to secure this information.

Most businesses and insurance markets are structured in a way that can magnify privacy concerns, notes John Means Cooper, VP of excess workers' compensation for AmWINS Brokerage of the Carolinas who moderated a SIIA national conference workshop on this topic. Since group health benefits are walled off from property and casualty insurance, risk managers and CFOs who handle the latter category aren't as familiar as HR executives with the Health Insurance Portability and Accountability Act (HIPAA), which isn't on their radar.

Work comp fund administrators already have their hands full fretting about the overall cost of medicine alongside a laundry list of other items. Data privacy concerns "won't even make the top 25," Cooper opines.

WRITTEN BY BRUCE SHUTAN

REGULATORY PATCHWORK

A similar disconnection also plays out along the regulatory landscape. For example, regulators in Pennsylvania's Department of Labor and Industry or the Louisiana Workforce Commission are work comp experts who don't understand other insurance lines, he says. Their concern is with ensuring that claims are properly handled and claimants are receiving the care they need. His point is that it would be up to state insurance commissioners to rule on cyber insurance or other matters related to protecting work comp data.

The regulatory landscape is daunting considering that in addition to complying with HIPAA, businesses also must still comply with statutes in all 50 states as well as industry-specific statutes and regulations. While some industry observers have suggested there will be some type of national data privacy breach law modeled after the General Data Protection Regulation in the European Union, it seems unrealistic in the U.S.


John Mullen

John Mullen, Sr., a partner with Mullen Coughlin LLC, recalls how in recent years 47 attorneys general implored Congress not to void their state privacy laws if a federal statute were passed. "My bet is that states wouldn't support a national law that knocked their laws off to the side," he predicts. "They probably would support one that, at some level, creates an awning effect in addition to their statutes."

Complying with a patchwork of state and federal data privacy laws is no easy undertaking. While there are a few federal laws that have some bearing as to data privacy and the handling of protected data, none have preemptive power, explains Megan North, AVP of professional liability for AmWINS Brokerage of Texas, Inc.

"Each state actually has its own laws about data privacy and what constitutes personal identifiable information, how that has to be protected, and if there's a potential breach of that data, then what actions need to be taken to rectify the situation," she says.

State attorneys general are becoming more involved with data privacy breaches, North reports. Their efforts include determining how sensitive information was compromised, preventing further incidents from occurring and levying penalties based on state regulations.

"We're going to see more scrutiny from regulators," she predicts, noting how all 50 states have enacted data privacy laws and some are already making revisions.

While poorly securing sensitive personal data is an unwise practice, Mullen explains that it doesn't necessarily violate privacy laws, calling it "more of a statutory compliance challenge if a privacy event occurs."

VULNERABLE CYBER TRAILS

A huge obstacle for self-insured work comp programs is the sheer number of times sensitive information changes hands. When Cooper starts the process of quoting someone's account, PII has been tossed from an insurance agent, carrier and third-party administrator through multiple email chains by the time it reaches him. It's then again shared with one or more carriers. In the never-ending transport of PII, he cautions that data is exposed to tremendous cyber risk.

Work comp data is a ripe target for sophisticated cyber criminals. "Hackers are looking for the easiest route with the biggest payoff, and medical records are going for quite a bit on the black market," North says.

Fewer than 20% of entities in the small to middle market (i.e., less than $500 million in revenue), depending on how it is defined, have purchased cyber insurance, according to Mullen, who ties that assessment to interactions with brokers and underwriters. "Five years ago, it was far lower," he adds.

YOUR BEST PARTNER LEADS THE WAY

For more than 35 years, self-funded employers have trusted Sun Life to deliver flexible stop-loss solutions and seamless claim reimbursement. And now, with our new Clinical 360 program, our clinical experts will review your claims data to identify cost savings and care optimization. With high-cost medical and pharmacy claims growing every year, you need your best partner with you every step of the way. **Ask your Sun Life Stop-Loss specialist about our latest innovations.**

STOP-LOSS | DISABILITY | ABSENCE | DENTAL/VISION | VOLUNTARY | LIFE

BRAD-6503k

SLPC 29427 02/19 (exp. 02/21)


Megan North

A baseline requirement in today's business world, Mullen notes that modestly priced cyber insurance premiums can buy millions of dollars in coverage and protection from "a panel of experts who do it fast and for a living." One reason why this product has such a low market penetration is because it's still a new line about which there's little awareness, Cooper notes.

Despite a muted market for cyber insurance, which some critics believe is overpriced, North notes that all industries are pushing to develop and test network security protocols or best practices to safeguard PII and PHI. She encourages companies to involve their employees in those activities, as well as empower them to speak up when something doesn't feel right.

Public pressure is one influential factor behind this movement. "I think people are starting to pay more attention to it, which is largely driven by expectations within our society," she adds. Another reason cyber security is top of mind is the need to protect an organization's reputation, especially in the highly competitive work comp space.

Ransomware is one rampant tactic that's being employed across every part of the economy. Under this frightening approach, hackers will threaten to release sensitive personal information to the public unless a specified amount of money is paid as a ransom. They do this by disguising a nefarious email that looks like it was generated by a legitimate source, but when a user clicks on the link, IT systems instantly freeze and can only be reactivated by the hacker or a cyber security expert who cracks the code.

"If you ask any of the major cyber insurers, they're going to tell you that's where they're largely getting hit right now because it's easy and quick," she says. "[Thieves are] sitting on a mine of extensive amounts of that data, and they might allege that they have it in their care."

RELYING ON EXPERTISE

What's crystal clear is that the self-insured work comp space will need to prepare for cyber security breaches in the future. There are nearly endless ways that cyber criminals can cobble together sensitive personal information, Cooper says.

They have become increasingly creative and sophisticated about poaching sensitive information, "and they will always eventually figure out a different way into something," he observes, noting how medical records are worth a fortune on the black market.

John Means Cooper

While not aware of any significant event involving work comp records, he cautions that it's only a matter of time before a TPA or other entity experiences

"some gigantic breach and loss, and that will wake everybody up." The trouble is that "insurance, by nature, is reactive and not a proactive industry," he adds.

The underwriting process helps corporate customers "become a better manager of data and better positioned to respond" to a data privacy event, Mullen says. Last year his law firm handled 1,200 such events alongside forensic teams of specialists who manage IT, insurance claims, credit and ID monitoring, public relations, etc., virtually any time of the day or night.

One common denominator he noticed in the self-insured workers' comp space is that those whose systems were penetrated often relied on internal IT staffers and in-house counsel. Depending on the facts, this strategy can turn "what should have been two or three days of a crazy forensic effort" into weeks of mop-up operations that worsened "until they finally reached out to their cyber insurer for help," Mullen reports.

Indeed, the need for specialization and independent expertise cannot be understated given the degree of complexity involved. "A lawyer who's a general practitioner or a business lawyer shouldn't be doing cyber breaches," says Mullen, whose team field cases each week from customers that aren't even aware that their servers are teeming with protected information. ■

Bruce Shutan is a Los Angeles freelance writer who has closely covered the employee benefits industry for more than 30 years.