BUSINESS INSURANCE®

JANUARY 20, 2014 www.businessinsurance.com $10

WORKERS COMPENSATION

SPECIALTY DRUGS DRIVE UP COMP COSTS

New hepatitis C treatment puts focus on price, usage of medications

BY SHEENA HARRISON

With a new hepatitis C drug entering the market at a cost of $1,000 a day and costs rising for other breakthrough pharmaceutical treatments, employers are seeing dramatic cost increases in workers compensation cases where the drugs are used.

"The cases are very rare but can be very expensive," said Dr. Teresa Bartlett, Troy, Mich.-based senior vice president of medical quality for Sedgwick Claims Management Services Inc.

The U.S. Food and Drug Administration granted approval last month to Sovaldi, a once-daily tablet prescribed to treat and cure hepatitis C. A 28-day supply of the pill carries a wholesale price of $28,000, Foster City, Calif.-based Gilead Sciences Inc., maker of Sovaldi, said in a statement.

Experts expect Sovaldi to be used in workers comp cases for workers exposed to blood-

See **DRUGS** page 28

HEALTH CARE REFORM

CFOs examine health care benefits through financial lens

BY JOANNE WOJCIK

Although the chief financial officer job in most organizations has been expanding as the cost of health care benefits consumes a growing portion of corporate budgets, health care reform is accelerating this evolution.

And as more CFOs become involved in benefits decision-making, they are showing greater interest in pay-or-play financial modeling, health benefits experts say.

In some cases, benefits advisers also are discovering the need to dispel some common misconceptions CFOs have about the Patient Protection and Affordable Care Act, sometimes having to remind them why their companies have been offering health benefits in the first place.

Nancy Kelly, managing partner and human capital practice leader at Hanover Stone Partners L.L.C. in New York, likened the change that has been occurring in the CFO's role to the emergence of the chief risk officer role in organizations.

"Now that the talent market is changing and is much more competitive, the CFOs have to become more involved in (the human resources) level so that they understand that simply taking the cost out of benefits isn't always the answer," Ms. Kelly said. "All of the executives have to cross borders. If you look at

See **CFO** page 28

RISK MANAGEMENT

Target strives to limit damage to reputation

Data breach highlights exposures retailers face

BY RODD ZOLKOS

Reputational risk experts give Target Corp. qualified good marks on the company's response to its holiday shopping season data breach, but acknowledge the picture could change for the retailer as more details emerge.

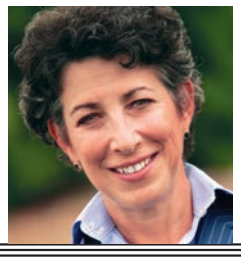
Meanwhile, broad awareness of the potential risks to the reputation of a company's brand exposed by cyber security issues is growing in the retail industry. Some experts even say such events could alter consumers' perceptions about the safety of e-commerce.

CYBER SECURITY
Read more on cyber security exposures
PAGE 3

In the days and weeks since its breach, Target has communicated with the stakeholders that hold the key to its reputation, though the event has had some discernable negative effect on its reputation, said Nir Kossovsky, CEO and director of Steel City Re, a Pittsburgh-based broker/adviser specializing in corporate reputation management and risk transfer.

"This is a firm that really has a chance to recoup that loss," Mr.

See **TARGET** page 26



Q&A: JULIE ROCHMAN
Head of the Insurance Institute for Business and Home Safety speaks out about building codes
PAGE 22

BENEFITS MANAGEMENT
As pension plans change, online retirement planning tools help engage workers
PAGE 8

RESEARCH & DATA
Ranking of the 20 largest underwriters of directors and officers coverage
PAGE 20

SPECIAL REPORT

D&O LIABILITY RISKS
LITIGATION DRIVER
Derivative shareholder lawsuits present D&O challenges; foreign shareholders filing D&O lawsuits in overseas courts; compensation rule could open new exposures; cyber risks pose big questions for executives.
PAGE 16

TARGET

Continued from page 1

Kossovsky said. "But it has not done a great job in communicating on the crisis management side. They left it open for others to control the story."

In the face of such a crisis, best practices in the immediate response are to demonstrate transparency, expertise, commitment, follow-up and empathy with affected customers, said Daniel Diermeier, IBM professor of regulation and competitive practice in the department of managerial economics and decision sciences of Northwestern University's Kellogg School of Management. "The key goal is to maintain or increase trust," he said.

"To my mind, Target did some of that, but not all of that," Mr. Diermeier said. "You have to do that quickly. Waiting until you know everything that happened often isn't an option for companies."

Target first acknowledged on Dec. 19 the data breach it experienced from Nov. 27 until Dec. 15, saying in a statement that the breach resulted in the theft of about 40 million credit and debit card records. On Dec. 27, the company said its forensic investigation found that hackers also collected card users' encrypted PIN data. On Jan. 10, the Minneapolis-based retailer said its investigation found that up to 70 million other records, including customer addresses and telephone numbers, had been stolen.

"Their response seemed pretty good and effective," said Larry Walsh, vice chairman at the Alexandria, Va.-based Hawthorn Group L.C., a strategic communications consulting firm. "But it took a long time for them to get there."

Since acknowledging the breach, Target has assured affected customers they'd have no liability for fraudulent charges. The third-largest U.S. retailer offered them one year of free credit monitoring and identity theft protection. The company also said last week it would testify before Congress in early February about the data breach.

As the investigation of the Target data breach continues, along with another one into a data breach that retailer Neiman Marcus acknowledged this month, retailer awareness is growing about the connection between cyber security and corporate reputation, experts say.

"The whole kind of data security area is emerging as — if not the main one — one of the more important drivers of reputational risk," said Mr. Diermeier, who also is director of the Ford Motor Co. Center for Global Citizenship at Northwestern's Kellogg School of Management. "The bigger you are, the more well known you are, the more likely you will find yourself in the spotlight."

Tom Kellerman, managing director at Alvarez & Marsal Holdings L.L.C. in New York, said: "Now that we're seeing a dramatic increase in reputational risk due to these events, the calculus has to change."

Historically, retailers relied too much on encryption and firewalls and not enough on next-generation cyber security strategies, he said, including both forensic capabilities and advanced threat detection capabilities.

Mr. Kellerman and others also emphasized the need to develop and test incident response plans companies can deploy when they've suffered a reputation-threatening data breach.

"One of the things you can do aside from all of the things (retailers) are doing on the technology side and the security side ... is to prepare for the response," said Tracy Knippenburg Gillis, global reputational risk and crisis management leader at Marsh Risk Consulting in New York. "That is really a huge difference in the way these things unfold, the reaction you see in the stakeholder groups."

Organizations should exercise their response plans, identify who will be involved and what they'll do, she said.

"There's no reason to be waiting until the time comes," Ms. Gillis said. "The faster you respond, the more accurate you are in your response, the better the outcome will be."

"We've seen a real dollar-for-dollar correlation of managing a crisis well," said Robert Parisi, network security and privacy practice leader at Marsh Inc. in New York. Reputational risk insurance can provide access to outside experts to help address such crises and help pay for their services, he said.

"You want to make sure that when an event occurs, you're getting out there with the right information," Mr. Parisi said. "Nothing is probably worse than getting out there saying nothing happened and then coming back and saying something happened."

With online communications and social media "the discretion, the ability to control (the story) is largely lost," said Hawthorn Group's Mr. Walsh, who advocates retailers and others handling large amounts of consumer information conduct data breach crisis drills at least once a year. Those who are prepared to act in real time will have the best chance of controlling the messages after a breach incident, he said.

Mr. Kossovsky said that the sort of mathematics applied to other risk exposures — weighing frequency and severity and determining "does the math justify the investment "— doesn't apply as well to decisions that might affect reputation.

"That's bad math when the risks are reputational," he said, because it ignores important intangible factors.

"The reputation issues are really best understood through another kind of math called game theory," Mr. Kossovsky said. "Your best decisions very much depend on how others are going to behave."

Mr. Diermeier said the increased awareness of reputational risk "has to become operational. It has to become part of your way of thinking."

A key question with potentially far-reaching implications is who consumers ultimately perceive as responsible for such a major data breach, said Kent Grayson, an associate professor of marketing at Northwestern's Kellogg School. "One question you want to ask about trust is who gets blamed," he said. In some instances it might not be the company involved in the event, but an institution.

"To what extent is Target going to be blamed for this vs. to what extent is electronic commerce going to be blamed as an institution?" Mr. Grayson said. "Who gets blamed; and if it's not Target but it's the institution of e-commerce, what are the implications of that?"

AP PHOTO

Target Corp. says about 40 million credit and debit card accounts may have been affected by a data breach during the holiday shopping season. The retailer carries $100 million in cyber liability insurance, sources say.

DATA BREACH CRISIS MANAGEMENT

Keys to managing data breach reputational threats are:

- **Control** the message by being the first and primary source of information on the breach.
- **Prepare** to respond immediately in real time with a fully integrated incident response plan.
- **Treat** affected individuals like family with prompt notification, credit monitoring and identity repair services, customer call centers.
- **Include** data breach scenarios in crisis planning/response drills and exercises.
- **Review** risk transfer options.

Source: The Hawthorn Group L.C.

Target has $100M in cyber cover, $65M D&O: Sources

Target Corp., which last month had a massive data breach that exposed the credit and debit card information of some 70 million customers, has at least $100 million of cyber insurance, including self-insured retentions, and $65 million of directors and officers liability coverage, according to insurance industry sources.

These well-placed sources, who requested anonymity, said Minneapolis-based Target is self-insured for the first $10 million of cyber coverage. On top of that, there's additional cyber insurance through: $15 million of excess coverage with Ace Ltd.; then a $15 million layer with American International Group Inc.; a $10 million layer with Bermuda-based Axis Capital Holdings Ltd.; another $10 million coverage layer with AIG; then a quota share for the next $40 million of cyber insurance divided among four unidentified insurers.

To protect against executive liability, the third-largest U.S. retailer has: a $10 million self-insured retention; followed by $25 million in primary D&O coverage with AIG; followed by an additional $15 million of coverage with Ace; and then $15 million of coverage with the Hartford, Conn.-based Travelers Cos. Inc.

On Dec. 19, Target said the data breach, during three weeks of the recent holiday shopping season, affected 40 million customers. Then on Jan. 10, the retailer said its investigation showed the breach was worse than anticipated and involved the theft of financial information of 70 million customers. That personal information, the retailer said, included PIN data embedded in customers' credits cards.

Target said its customers will have no liability for fraudulent charges resulting from the data breach. The breach has triggered state and federal investigations, as well as several lawsuits against Target.

Target declined to comment on its cyber and D&O insurance coverage. A Travelers spokeswoman said in a statement the insurer cannot confirm whether anyone is a client. An Ace spokeswoman said in a statement: "As a matter of company policy and confidentiality, we do not comment on specific claim incidents and cannot confirm or deny coverage with any particular company." AIG declined to comment. An Axis representative could not be reached for comment.

By Judy Greenwald