There are many rankings of companies based on their good qualities, such as most admired, most trustworthy, best to work for, most ethical, and so on, yet there are few formal rankings of companies that act unethically or develop a poor reputation. An exception is the work of 24/7 Wall St., which for the past three years has evaluated large companies and high-profile brands in the United States to determine the year’s “Nine Most Damaged Brands.”

General Motors topped the list this year because of the allegations that the automaker knowingly sold cars that had defective parts or systems. According to The Wall Street Journal, the cost of GM’s massive recall of cars due to a faulty ignition switch may reach $7 billion. A key determinant of the final cost is whether incidents that occurred prior to GM’s 2009 bankruptcy can be included in lawsuits against the company.

The major ethics issue in the GM ignition switch safety scandal involves a potential cover-up of the problem for many years. Customers reported problems with their vehicles stalling—a symptom of the defect—as early as March 2005. In September 2005, an engineering estimate indicated the cost to change the switch would be $0.90 per vehicle plus an investment of $400,000 in production machinery. This information was circulated within the company, but, apparently for cost reasons, the decision was made to not recall and repair any cars already sold.

In 2006, the engineer responsible for the design of the ignition switch requested the part supplier to change the design of the switch without changing the part number. Apparently, records of the design change and the reasoning for not changing the part number were lost until 2013. At that point, a GM internal investigation showed that a driver’s knee could cause the ignition to turn off, resulting in the failure of critical safety functions such as braking, steering, and even air-bag deployment. The U.S. Department of Transportation fined the company $35 million (the maximum allowable) for its failure to promptly advise the National Highway Traffic Safety Administration (NHTSA). According to NHTSA Acting Administrator David Friedman, “GM engineers knew about the defect. GM investigators knew about the defect. GM lawyers knew about the defect. But GM did not act to protect Americans from that defect.” GM will pay for this inaction in the courts.

The major lesson from GM is that an open and ethical culture within an organization that allows problems to be acknowledged and solved earlier rather than later is likely to result in superior long-term financial performance. As a partial solution to the ignition switch problem, GM has initiated a “Speak Up for Safety” program to motivate employees to come forward with problems rather than keeping silent. GM Chair and CEO Mary Barra said, “GM must embrace a culture where safety and quality come first. GM employees should raise safety concerns quickly and forcefully, and be recognized for doing so.”

Another company on the 24/7 Wall St. list is Target. The massive security breach it experienced in November 2013 exposed the personal information of as many as 70 million people. Information Technology (IT) professionals...
provide the expertise for securing the organization’s IT assets. In fact, Target reportedly used a malware detection tool from FireEye, a developer of threat protection software. The software had picked up on sketchy behavior several weeks before the breach became public, yet Target failed to act forcefully.

An article in the February/March 2014 issue of Security Technology Executive, “The Target Breach—Can It Be Prevented?” describes how easy it was for the seemingly unsophisticated wrongdoers to act:
◆ “A phishing attack against Fazio Mechanical Services, Target’s refrigeration contractor—that was apparently using the free Malwarebytes Anti-Malware software that failed to protect it against the ensuing malware.”
◆ “Login credentials issued by Target to Fazio Mechanical Services were obtained by the criminal hackers which provided subsequent network access (via a Web portal) into the Target environment.”
◆ “Point-of-sale (POS) malware—presumably the BlackPOS available for purchase online—was uploaded to POS systems at Target stores and used to scrape credit card information and related information directly from the memory of the POS computers,” where it only exists for a short time.

The fact that management apparently took no action despite FireEye’s advanced warning may not be unusual. “The Target Breach” reports the results of a survey by AccessData and the Ponemon Institute, which found that “36% of IT security pros would tell the CEO and board of directors that a cyberattack had been resolved even if they didn’t know that it had been.” This lack of open communication within an organization and failure to report unfavorable events is a symptom of a weak ethical culture that allows bad news to be kept under cover rather than being resolved. Target apparently didn’t have an incident response plan, so it was unprepared to act quickly when presented with a critical event. The consequences for Target were immediate and extensive. Sales and profits declined, the company’s share price fell about 11%, and the CIO and other key IT professionals were forced to resign almost immediately.

But it didn’t end there. Target’s board chair and CEO resigned on May 2. And later in May, The Wall Street Journal reported in “ISS’s View on Target Directors Is a Signal on Cybersecurity” that a prominent proxy advisory service to large investors “called on Target shareholders to oust seven of the company’s 10 directors for not doing enough to ensure Target’s systems were fortified against security threats.” The seven were members of the audit and corporate responsibility committees, deemed most responsible for the oversight of risk. Target and its shareowners likely face further pain in the form of civil suits.

The major lesson to be learned from Target’s disaster is the same as in GM’s case: It’s absolutely necessary to have an ethical climate that allows communication within the organization about adverse events as well as good news. Had the companies responded to the available information, the situations could’ve been avoided or the damage to their brand minimized.

Last year’s list of the nine most damaged brands directly involved ethics issues as well—Hyundai and J.P. Morgan Chase. The South Korean automaker Hyundai made great strides between 2001 and 2011, increasing its market share in the U.S. from only 2% to 4%. Hyundai and its sister brand Kia offered good-value, high-quality vehicles at an affordable price. And the “Hyundai Assurance” 100,000-mile warranty was a special selling point. But in the end, Hyundai breached the public’s trust. The bad news struck in November 2012 when the U.S. Environmental Protection Agency (EPA) asserted Hyundai had overstated its claimed gas mileage performance and was forced to lower the miles-per-gallon numbers stated on many of its vehicles. The company’s response damaged the brand further. It attempted to describe itself as a

For guidance in applying the IMA Statement of Ethical Professional Practice to your ethical dilemma, contact the IMA Ethics Helpline at (800) 245-1383 in the U.S. or Canada. In other countries, dial the AT&T USA Direct Access Number from www.usa.att.com/traveler/index.jsp, then the above number.
consumer champion rather than having been caught by the EPA misleading the public.

J.P. Morgan Chase’s case involved the famous “London Whale,” a trader in the London branch whose actions cost the bank $6.2 billion. The trader took large positions in the market for credit default swaps. The Securities & Exchange Commission (SEC), Commodities Futures Trading Commission (CFTC), and bank regulators exacted an admission of wrongdoing on the part of the bank and assessed penalties of $800 million. The bank admitted to having inadequate internal controls and to improperly disclosing information to investors and the public.

Ethics isn’t only about knowing what’s right and wrong and doing the right thing. Ethics also involves acting with responsibility, considering objectivity when making decisions, putting forth honesty in all relationships, and employing fairness as a critical criterion. The IMA Statement of Ethical Professional Practice demands professional accountants behave in accordance with these principles. The companies on the 24/7 Wall St. list didn’t follow these important concepts. They now face monetary fines, possible lawsuits, and significantly damaged reputations. SF

Curtis C. Verschoor, CMA, CPA, is the Emeritus Ledger & Quill Research Professor, School of Accountancy and MIS, and an honorary Senior Wicklander Research Fellow in the Institute for Business and Professional Ethics, both at DePaul University, Chicago. He also is a Research Scholar in the Center for Business Ethics at Bentley University, Waltham, Mass. He was selected by Trust Across America—Trust Around the World as one of the Top Thought Leaders in Trustworthy Business—2014. John Wiley & Sons has published his latest book, Audit Committee Essentials. His e-mail address is curtisverschoor@sbcglobal.net.

Ethics continued from page 12