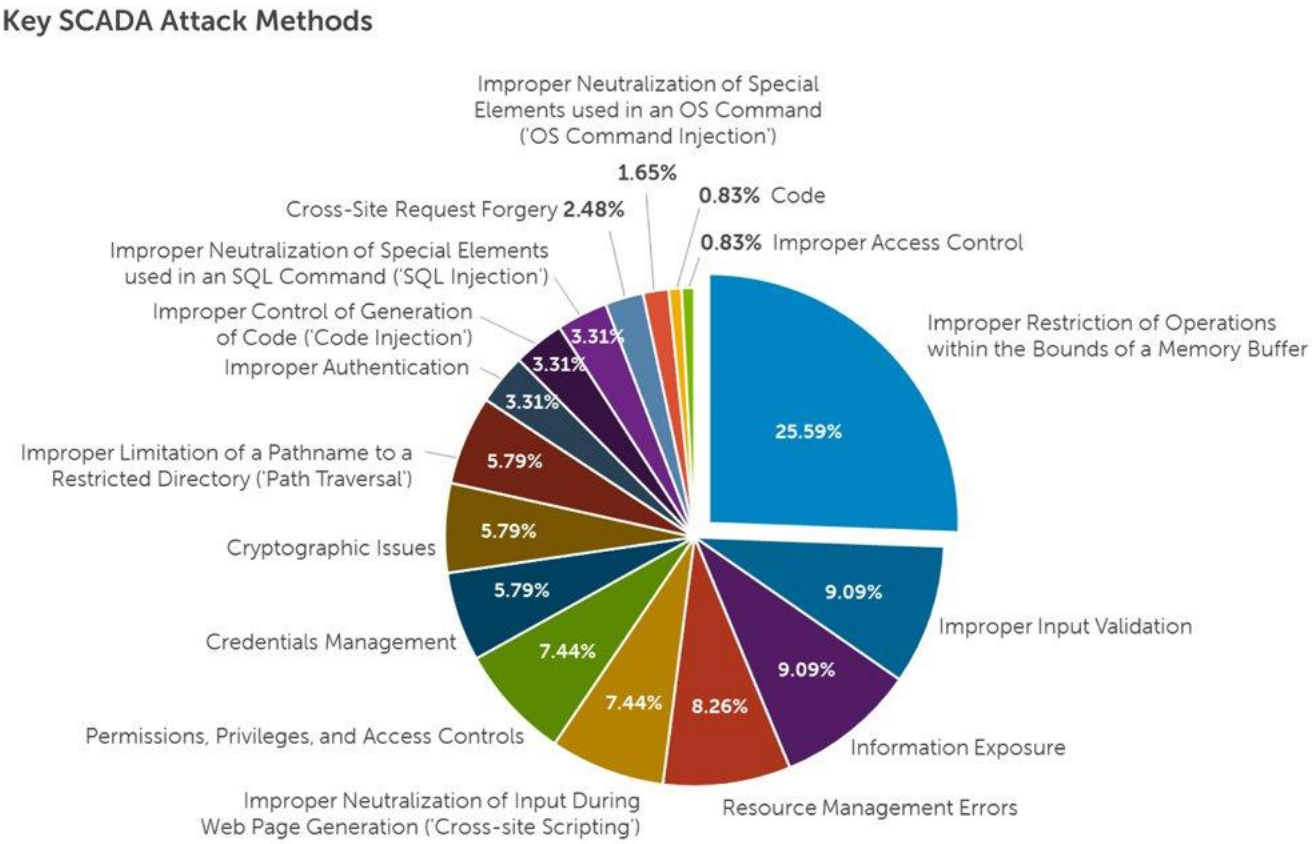
SCADA Attacks Double in 2014

Dell Security's annual threat report shows not only a significant surge in the number of attacks on retail credit card systems, but industrial SCADA systems as well, which are much more likely to go unreported.



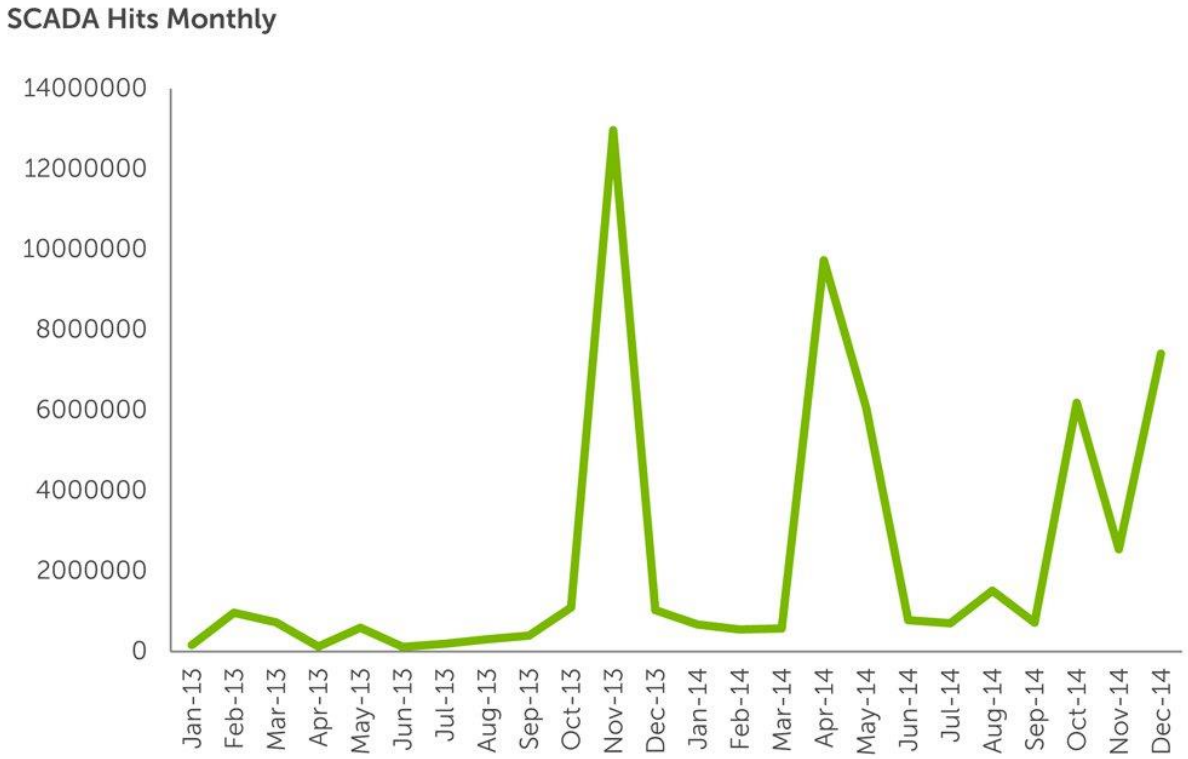
For Dell to report an annual surge in point-of-sale (POS) attacks aimed at payment card infrastructures might not be such a surprise to people who pay any attention to the news. We know that the retail industry was hit hard by cybersecurity attacks in 2014—Target wasn't the only target, so to speak, though it got the year started, and was the largest breach in the history of U.S. retail until Home Depot was hit even harder later in the year. There were also significant attacks on Michaels, Staples, Goodwill and more.

Significant bearing on process industries

But don't be thinking that the attacks are just focused there. What Dell also found in its annual threat report was that the number of attacks on SCADA systems doubled from 2013 to 2014. Obviously, that has significant bearing on process industries, which use SCADA systems to control remote equipment and collect data on that equipment's performance.

As industrial manufacturers face threats, other companies within the same space might not even know a SCADA threat exists until they are targeted themselves. "Since companies are only required to report data breaches that involve personal or payment information, SCADA attacks often go unreported," said Patrick Sweeney, executive director for Dell Security. "This lack of information sharing combined with an aging industrial machinery infrastructure presents huge security challenges that will to continue to grow in the coming months and years."

Unlike the retail breaches, which are likely geared toward financial gain, attacks against SCADA systems tend to be political in nature, targeting operational capabilities within power plants, factories and refineries.



Dell's annual threat report relies on research from its Global Response Intelligence Defense (GRID) network and telemetry data from Dell SonicWall network traffic to identify emerging threats. For SCADA systems, buffer overflow vulnerabilities continue to be the primary point of attack, according to the Dell SonicWall Research Team, accounting for a quarter of the attacks.
The majority of the SCADA attacks targeted Finland, the UK and the U.S. One likely reason for that, however, is that SCADA systems are more common in these regions and more likely to be connected to the Internet. In 2014, Dell saw 202,322 SCADA attacks in Finland; 69,656 in the UK; and 51,258 in the U.S.

Along with the doubling of SCADA attacks from 2013 to 2014, a look at January numbers alone shows a staggering rise, year over year. Worldwide SCADA attacks increased from 91,676 in January 2012 to 163,228 in January 2013, and 675,186 in January 2014.

Make sure all software and systems are up to date
"Everyone knows the threats are real and the consequences are dire, so we can no longer blame lack of awareness for the attacks that succeed," Sweeney said. "Hacks and attacks continue to occur, not because companies aren't taking security measures, but because they aren't taking the right ones."
Dell recommends a few general ways to protect against SCADA attacks. For one, make sure all software and systems are up to date. "Too often with industrial companies, systems that are not used every day remain installed and untouched as long as they are not actively causing problems," Dell's report explains. "However, should an employee one day connect that system to the Internet, it could become a threat vector for SCADA attacks."

Make sure your network only allows connections with approved IPs; and follow operational best practices for limiting exposure, such as restricting or disabling USB ports and Bluetooth.
Dell also urges manufacturers to report and share information about SCADA attacks to help ensure the industrial community as a whole is appropriately aware of emerging threats.

Mobile security
As mobility continues to take hold in the manufacturing space and the bring-your-own-device (BYOD) trend grows, it's worth noting another section of Dell's threat report focused on sophisticated, new malware techniques targeting smartphones. "Smartphone attacks have been a security concern since mobile devices began to reach widespread adoption, but it wasn't until 2014 that smartphone malware began to look and act like its desktop predecessors," Dell's report notes. Both Android and iOS malware took hold in 2014, and Dell expects malware to emerge this year targeting wearables, televisions and other ancillary devices. "The pairing of these devices to laptops and smartphones will give hackers an easy attack vector, and these devices will become much more enticing as the market grows in the coming months," the report details.

Common factors
Though Dell's report details several key findings in a variety of industries and attack points, there were some key common denominators. For example, several of the breaches throughout the year involved companies that overlooked one or more basic threat vectors: outdated, unpatched software; under-restricted contractor access to networks; under-secured network access for mobile or distributed users; and under-regulated Internet access for all employees.

"Some of these threat vectors have posed security challenges for years, while others are emerging as a result of today's highly mobile, consumer-tech-empowered workforce," the report says. "As always, cyber criminals remain adept at finding new ways to exploit common blind spots and even use companies' best security intentions against them."

The most effective approach manufacturers can take is a defense-in-depth program, Dell concluded, establishing multiple layers of security and threat intelligence for preventing and responding to attacks on the network.