AS THE CLOCK strikes midnight on the new year, so begins the countdown to a new round of security threats and breaches that doubtless will unfold in 2015. But this year will be a little different. In the past, when we’ve talked about threat predictions, we’ve focused either on the criminal hackers out to steal credit card data and banking passwords or on the activist hackers out for the lulz (and maybe to teach corporate victims a lesson).

But these days, no threat predictions are complete if they don’t address the looming threats posed by nation-state attacks, like the ones exposed by Edward Snowden. It’s been said repeatedly that when a spy agency like the NSA undermines a system to gain access for its own use, it makes that system more vulnerable to attack by others. So we begin this list with that in mind.

**Nation-State Attacks**

We closed 2014 with new revelations about one of the most significant hacks the NSA and its partnering spy agency, the UK’s GCHQ, are known to have committed. That hack involved Belgium’s partly state-owned telecom Belgacom. When the Belgacom hack was first exposed in the summer of 2013, it was quickly hushed up. Belgian authorities made nary a sound of protest over it. All we knew was that the spy agencies had targeted system administrators working for the telecom in order to gain access to special routers the company used to manage customer cell phone traffic. New revelations about the Regin malware used in the hack, however, show how the attackers also sought to hijack entire telecom networks outside of Belgium so they could take control of base stations and monitor users or intercept communications. Regin is clearly just one of many tools the spy agencies have used to undermine private company networks. These and other efforts the NSA has employed to undermine encryption and install backdoors in systems remain the biggest security threat that computer users face in general.

**Extortion**

Controversy still swirls around the Sony hack and the motivation for that breach. But whether the hackers breached Sony’s system to extort money or a promise to shelve The Interview, hacker shakedowns are likely to occur again. The Sony hack wasn’t the first hacker extortion we’ve seen. But most of them until now have occurred on a small scale—using so-called ransomware that encrypts a hard drive or locks a
user or corporation out of their data or system until money is paid. The Sony hack—possibly perpetrated by hacktivists aided by a disgruntled insider or nation-state-backed hackers, according to the government and various alternative theories—is the first high-profile extortion breach that involved threats of data leaks. This kind of hack requires more skill than low-level ransomware attacks, but could become a bigger problem for prominent targets like Sony that have a lot to lose with a data leak.

**Data Destruction**

The Sony hack announced another kind of threat we haven’t seen much in the U.S.: the data destruction threat. This could become more common in 2015. The attackers behind the breach of Sony Pictures Entertainment didn’t just steal data from the company; they also deleted it. It’s a tactic that had been used before in attacks against computers in South Korea, Saudi Arabia and Iran—in South Korea against banks and media companies and in Saudi Arabia and Iran against companies and government agencies involve in the oil industry. Malware that wipes data and master boot records to render systems inoperable. Good data backups can prevent an attack like this from being a major disaster. But rebuilding systems that are wiped like this is still time-consuming and expensive, and you have to make sure that the backups you restore are thoroughly disinfected so that lingering malware won’t re-wipe systems once restored.

**Bank Card Breaches Will Continue**

In the last decade there have been numerous high-profile breaches involving the theft of data from millions of bank cards—TJX, Barnes and Noble, Target and Home Depot to name a few. Some of these involved hacking the point-of-sale systems inside a store to steal card data as it traversed a retailer’s network; others, like the Barnes and Noble hack, involved skimmers installed on card readers to siphon card data as soon as the card was swiped. Card issuers and retailers are moving to adopt more secure EMV or chip-‘n’-PIN cards and readers, which use an embedded microchip that generates a one-time transaction code on in-store purchases and a customer-entered PIN that makes stolen data less useful to card thieves. As a result, card breaches like this are expected to decline. But it will take a while for chip-‘n’-PIN systems to be widely adopted.

Though card issuers are slowly replacing old bank cards with new EMV cards, retailers have until October 2015 to install new readers that can handle the cards, after which they’ll be liable for any fraudulent transactions that occur on cards stolen where the readers are not installed. Retailers no doubt will drag their feet on adopting the new technology, and card numbers stolen from older DNV cards can still be used for fraudulent online purchases that don’t require a PIN or security code. There’s also a problem with poor implementation; cards stolen in the recent Home Depot hack show that hackers were able to exploit chip-‘n’-PIN processing systems because they were poorly implemented. With the shift to EMV cards, hackers will simply shift their focus. Instead of going after retailers for card data they’ll simply target card processors that handle payroll accounts. In recent hacks involving the theft of $9 million and $45 million, hackers broke into the networks of companies responsible for processing pre-paid card accounts for payroll payments. After artificially increasing the balance and withdrawal limit on a handful of payroll accounts, mules around the world then cashed out the accounts through hundreds of ATM withdrawals in various cities.

**Third-Party Breaches**

In recent years we’ve seen a disturbing trend in so-called third-party hacks, breaches that focus on one company or service solely for the purpose of obtaining data or access to a more important target. We saw this in the Target breach when hackers got into the retailer’s network through a heating and air-conditioning company that did business with Target and had access to its network. But this is low-level
compared with more serious third-party breaches against certificate authorities and others that provide essential services. A breach against RSA Security in 2011 was aimed at getting the hackers access to RSA security tokens used by government agencies and corporations to secure their systems. And a breach of certificate authorities—such as one involving a Hungarian certificate authority in 2011—provides hackers with the ability to obtain seemingly legitimate certificates to sign malware and make it look like legitimate software. Similarly, a breach of Adobe in 2012 gave the attackers access to the company’s code-signing server, which they used to sign their malware with a valid Adobe certificate. Third-party breaches like these are a sign that other security measures have increased. Hackers need to resort to stealing certificates because operating systems like Windows now come with security features that prevent certain code from installing on them unless it’s signed with a legitimate certificate. These kinds of breaches are significant because they undermine the basic trust that users have in the internet’s infrastructure.

**Critical Infrastructure**

Until now, the most serious breach of critical infrastructure we’ve seen occurred overseas in Iran when Stuxnet was used to sabotage that country’s uranium enrichment program. But the days when critical infrastructure in the U.S. will remain untouched are probably drawing to a close. One sign that hackers are looking at industrial control systems in the U.S. is a breach that occurred in 2012 against Telvent, a maker of smart-grid control software used in portions of the U.S. electrical grid as well as in some oil and gas pipeline and water systems. The hackers gained access to project files for the company’s SCADA system. Vendors like Telvent use project files to program the industrial control systems of customers and have full rights to modify anything in a customer’s system through these files. Infected project files were one of the methods that Stuxnet used to gain access to Iran’s uranium-enrichment systems. Hackers can use project files to infect customers or use the access that companies like Telvent have to customer networks to study the customer’s operations for vulnerabilities and gain remote access to their control networks. Just like hackers used third-party systems to gain access to Target, it’s only a matter of time before they use companies like Telvent to gain access to critical industrial controls—if they haven’t already.

http://www.wired.com/2015/01/security-predictions-2015/