Ah, 2016 – the year of fake news, celebrity deaths and cyberattacks, namely to the electricity grids of several countries. The biggest story came out of the United States, where *The Washington Post* (falsely) reported that a Vermont utility had been infiltrated by Russian hackers.

Should energy managers be concerned about cyberattacks like these? Embracing connectivity thanks to the IoT devices of Industry 4.0 also means exposing buildings to potential security vulnerabilities, a significant fear among facility managers. In this article, we'll examine which energy data security issues facility managers should be aware of, and most importantly, how to protect against them.

Smart grid security: An overblown threat?

Let's circle back to our utility in Vermont. Because the infected computer wasn't actually connected to the grid, *The Washington Post* later admitted the story had been reported incorrectly. Still, American electricity infrastructure is said to be under "imminent threat" according to numerous other reports of China, Russia and other nations attempting to deploy malware reaching as far back as 2009.

The United States is not the only country facing energy-related security threats. Ukraine suffered a major energy data security breach in December 2015 that destabilized the power grid and caused blackouts in parts of Kiev. More than 6,500 cyberattacks were carried out on Ukrainian government institutions over a 2-month period last year. Turkey and Israel also experienced significant attacks last year, leading to the paralysis of several machines within the electricity authorities of those countries.

This recent rise in cyberattacks on smart grids might raise concerns among energy managers, who are stuck between a rock and a hard place when it comes to keeping pace with technological evolution while combating the increased risk of vulnerabilities. As the digital transformation of the grid progresses, the frequency and severity of security threats increases with it. But what about energy data security at the building level?

The hard truth is this: Anything and everything with an internet connection is inherently vulnerable to hacking. As the Internet of Things expands and we move closer to Industry 4.0, it's no wonder energy managers in charge of thousands of meters and sensors all connected to the cloud are concerned. In the next section, we'll take a look at how data security is managed at the building level, and what to do if yours has been compromised.

Energy data security in buildings

Cyberattacks on buildings can take many forms, from pure data theft to sabotaging or disrupting a building's activities. If you already have an energy management software

system installed, be ready to accept the fact that targeted malware will increasingly be able to control and manipulate building processes: a natural next step in the constant evolution of malware.

For example, if a machine running a building management system with control capabilities becomes infected, the malware can determine which systems it can manipulate, down to the end device level. Depending on the type of building you are operating, the consequences can be dangerous.

In smart buildings, enormous amounts of device-level data flow from sensors and meters (that detect changes in temperature, humidity, presence, etc.) into some kind of central management hub, such as an Energy Management Software, or EMS, platform.

Smaller buildings such as individual homes only have a few smart appliances, such as intelligent fridges or washing machines, and usually don't need a full-scale energy management solution. On the other hand, industrial buildings with BMS or SCADA systems to control manufacturing processes, are practically required to manage their energy data due to the sheer volume and resulting impact on the bottom line. Buildings or factories that are large enough to generate their own energy and sell it back to the grid are also becoming increasingly commonplace, especially with the advancement of both smart meters and demand response technology.

How can I ensure my energy data is available and secure?

First, don't fall for the myth that SaaS is insecure by nature. Just because your data resides in the cloud doesn't mean it won't be subject to rigorous security protocols.

For some first-time SaaS buyers, this still isn't enough to quell their fears of the cloud, and they end up insisting on on-premise energy management. As the managing director of a leading Italian energy service company notes:

"This is the first question I get from my prospective clients. Their number one pain point is worrying about how secure their data will be in the cloud. But, as soon as I show them the safety and reliability protocols built into DEXCell Energy Manager, they agree to proceed."

Second, aim to work with a proven, trusted energy management software vendor that is well-established on the market. If you are in the middle of a procurement process, security is among the top 10 essential questions you should ask potential vendors before buying any automatic monitoring and targeting software. Is there a failsafe protocol? What is the backup frequency? What about the update process? Are reboots required?

After doing your research, go for the solution that explicitly includes leading edge, promising security technology. For "systems of systems" like energy management platforms, having a solid, secure way to update devices is of utmost importance and

gives lots of flexibility, says cybersecurity expert Billy Rios of WhiteScope LLC: "If your potential vendor starts talking about security updates via USB key, RUN AWAY!"

If you are already working with an energy analytics platform start to notice weird things happening with your energy data, what should you do?

What are my options if I think my data has been compromised?

The first hours following any breach are the most critical, so your immediate concern is to focus on some kind of action plan.

If you have serious reason to believe that your energy management system has been hacked, here are a few steps data security experts recommend you to take:

Communicate internally: Don't wait to inform management and document everything (who, what, where, when, how) to help further investigation and to avoid future issues: create screenshots, disk images and notes to help your IT support team figure out what happened, fix it, and prevent it in the future.

Contain the threat: Once you have identified which and how many machines have been compromised and reported the breach, form a task force to stop it. If that means bringing in external data security specialists to isolate the infected system, so be it – all resources should be used to stop the breach.

Communicate externally: As soon as the problem is under control, determine who needs to be informed. Work with your legal and PR departments to ensure that the necessary outside parties (clients, especially if you are an energy services company) are notified properly. Create a proactive incident response plan together with your EMS provider that is tested frequently to make sure any flaws are fully resolved. Review server logs and run penetration tests periodically, making sure to investigate whether other servers are susceptible.

Joan Pinyol is the co-founder and CEO of DEXMA, a leading provider of cloud-based energy analytics software for commercial buildings, industrial facilities and large property portfolios. Based in Barcelona, DEXMA is the preferred energy management partner for more than 200 ESCOs, utilities and integrators around the world that form our Global Partner Network. A version of this column originally appeared on DEXMA's blog.