# The Russian Cyberattack That Never Was

**Posted on** Monday, January 16, 2017

Concerns about Russian state-sponsored hacking reached a new peak last week as allegations were made about a security breach at a Vermont utility provider. The discovery of malware in the Burlington Electric Department network immediately prompted accusations that Russia was behind the attack – and the media went mad.

Coming so soon after President Obama's own claims that Russia interfered with the US election, many 'outraged' American politicians moved quickly to denounce the actions of foreign hackers. The Governor of Vermont, Peter Shumlin, was particularly quick off the mark, saying;

"Vermonters and all Americans should be both alarmed and outraged that one of the world's leading thugs, Vladimir Putin, has been attempting to hack our electric grid, which we rely upon to support our quality-of-life, economy, health, and safety."

Embarrassingly these claims turned out to be unfounded.

As the forensic investigation continued in Vermont, it became clear that the "hack" was not state sponsored at all. In fact, the whole event was triggered by a single employee checking their Yahoo email account from a malware-infected laptop. Inspection revealed that far from a sophisticated attempt by Russia to compromise the US energy network, one user had fallen victim to some unsophisticated "script kiddies" out to steal his personal data.

## One false alarm among many genuine breaches

Although the incident at Burlington clearly wasn't part of some master plan to take over the US power grid, there were plenty of genuine cyberattacks taking place last year. According to one estimate provided by Lewis Morgan on the IT Governance blog, there were at least 3.1 billion records leaked in 2016 – 1 billion of which came from Yahoo! alone.

Clearly this is a worrying state of affairs, both for customers who have their personal data stolen, and for businesses who will be called to account for these lapses in security.

State sponsored or otherwise, cybersecurity breaches are becoming more, not less, common. So as 2017 picks up speed, CTOs need to seriously consider how they are going to improve the security of their systems and data – and spend accordingly.

## Next steps

Need someone to make sure your hardware is working effectively? **Please get in touch with us**.