Nuclear Station Suffers USB Data Breach

The data breach threat posed by USB sticks has once again been exposed after nuclear processing company Sellafield began an investigation into the loss of a USB device, said to contain information about its business operations.

The USB device was found in a hotel room at the Ennerdale Country House Hotel in Cumbria by coach driver Craig Beavan.

The data was reportedly unencrypted and included details of a proposed workforce transfer and the benefits of the staff transfer, including lower costs and reduced liabilities. There was also information on the stick that suggested that the International Atomic Energy Agency technicians visiting the site were not sufficiently briefed on health and safety regulations.

Investigation Launched

Beavan said that he found the stick on the floor of his room at the hotel and then checked its contents on his computer to identify who it belonged to.

“I was coming out of the bathroom and saw it on the floor, I put it in my computer to see who it belonged to when I found the Sellafield documents,” Beavan told the Whitehaven news. “I couldn’t believe it. It is more what could have been on the stick that bothers me. There might not be anything top secret on there but what if there had been? I am concerned it was left there, anyone could have found it.”

Sellafield has said that it is investigating how the stick came to be left in the hotel room.

“Sellafield Ltd understands there is no sensitive material on the memory stick. However, we take this issue very seriously and are investigating how this happened,” a spokesman was quoted as saying by the Whitehaven news.

It is thought that Sellafield provides its staff with USB memory sticks in order to transfer business related information. “All users of USB memory sticks are provided with guidance on their use. We control sensitive nuclear information in line with strict security regulations,” the spokesman said.

Not The First Time

This is not the first time that a USB stick has caused a data breach. In early September a memory stick said to contain anti-terror training manuals was discovered outside a Manchester police station. In May, a NHS worker in the secure mental health unit of a Scottish hospital was suspended, after he lost a USB stick containing patients’ medical records. More recently a healthcare agency (Healthcare Locums Plc) was found to be in breach of the Data Protection Act (DPA) after it lost a hard disc drive (HDD) that contained personal data of the doctors it employed,

such as their security clearances and visa information.

This latest loss provoked a quick reaction from data security specialists.

“While the convenience of USB sticks make them an important tool for any business, you don’t have to be a nuclear scientist to know that the data carried on these devices must be protected,” Sean Glynn, vice president and chief marketing officer at Credant Technologies.

Encryption Needed

“Corporate USB sticks should always include encryption and other forms of security as a basic requirement because – as this incident clearly shows – unencrypted data can, and does, fall into the wrong hands,” said Glynn.

“Sellafield has done the right thing in launching an investigation, but this is a potentially serious breach of data security on several levels, with national security overtones. Sellafield needs to look very carefully at its data security policies, and the technology that enforces those policies,” said Glynn.

Data breaches of this kind fall under the remit of the Information Commissioner’s Office.

The ICO has previously warned businesses that if they do not own up to data breaches, they will face tougher action than those that come forward of their volition. Companies that fall foul of data breach laws risk a maximum fine of £500,000 under powers granted to the ICO in January this year.