Insulin pump maker identified after hacking talk

25 August 2011, By JORDAN ROBERTSON , AP Technology Writer

In this file photo taken Aug. 4, 2011, Jay Radcliffe, who wrote a program to attack an insulin pump and taking control of the device wirelessly, is pictured at the annual Black Hat conference for digital self defense, in Las Vegas. (AP Photo/Isaac Brekken, File)

(AP) -- When Jay Radcliffe revealed three weeks ago that he'd found serious security holes in a popular type of insulin pump that diabetics wear, he kept two important details secret: the pump maker's name, and the specific technique he used to hack the device.

The problems he found carry exceptional risks, such as being able to program a special remote control to command strangers' pumps to dispense the wrong dosage of insulin. But Radcliffe said he was ignored in repeated attempts to alert the company to the defects. On Thursday he identified the company - Medtronic Inc. - in an effort to apply public pressure to fix the vulnerabilities.

The disclosure raises the risk of attacks on certain Medtronic insulin pumps. But Radcliffe said he hopes that exposure helps fix the problems. He said he tried to handle the disclosure ethically - by working with the company first - and felt "there should have been an ethical response (from the company) to that."

Radcliffe, a diabetic who experimented on his own Medtronic pump, revealed the details to The Associated Press ahead of a planned news conference.

Medtronic would not directly address its interactions with Radcliffe. Spokeswoman Amanda Sheldon said a Medtronic employee attended Radcliffe's presentation at the Black Hat computer security conference this month in Las Vegas and said the company was analyzing his public statements.

"We have to evaluate the sources of the information and figure out what we should do with it," she said.

Radcliffe said his public statements intentionally lacked the specific technical details that Medtronic would need to address the vulnerabilities he's found. After the Department of Homeland Security, which examined his research, helped make the introduction to Medtronic, his calls and e-mails went unanswered, he said, a claim Medtronic wouldn't specifically address.

Radcliffe, who lives in Meridian, Idaho, said the experience has caused him to switch to another company that appears to use stronger security.

However, he said Medtronic customers should continue to use their pumps, as the techniques he developed are hard to execute in the real world - for now. Hacking attacks tend to get easier as more people do them, because hackers can write programs to automate the most cumbersome tasks.

The tension is more than an inside-baseball ethical dilemma about how security professionals should deal with companies they believe have been uncooperative and aren't fixing known vulnerabilities.

Medtronic, which is based in Minneapolis, is one of the world's biggest medical device makers. A Medtronic device that works as a pacemaker and

defibrillator was also found in a different study in 2008 to be vulnerable to hacking attacks.

Radcliffe's findings and the earlier study are examples of hacking attack of the future, in which the sophisticated software and communications chips being added to everyday technologies will make them vulnerable to frightening new attacks.

Medical devices are particularly vulnerable because there are clear advantages in allowing them to talk to each other wirelessly and connect to the Internet. That connection allows devices to receive important software updates, and it lets patients upload their medical information to special websites to track the status of their conditions. But medical device makers aren't used to hackers picking apart their products, and there's no clear path for disclosing weaknesses.

In light of Radcliffe's findings, two lawmakers, Reps. Anna Eshoo of California and Edward Markey of Massachusetts, both Democrats, have asked the Government Accountability Office, the investigative arm of Congress, to evaluate the government's efforts to identify the risks of implants and other medical devices that use wireless communication.

Radcliffe said he also took issue with a statement that Medtronic issued after his presentation. The company had asserted that turning off the device's wireless function would protect users from attack. Radcliffe said that statement is inaccurate because the particular wireless ability he exploited can't be turned off, which means a deeper fix would be needed.

Sheldon, the Medtronic spokeswoman, would not address Radcliffe's claims specifically, saying that "we're not going to bit-by-bit outline our security measures." She added that the "risk of deliberate, malicious or unauthorized manipulation of our insulin pumps is extremely low" and that the company is not aware of any attacks on its devices outside of research environments.

Sheldon said the company is open to talking to Radcliffe. Radcliffe said he received an email from Medtronic's public relations department after a reporter inquired about the issue.