Looking Back: Still Not Serious About Online Security

By Erika Morphy | *Dec 30, 2015*

Published by CMSWire http://www.cmswire.com/information-management/looking-back-still-not-serious-about-online-security/?pageNum=1

After the horrific terrorist attacks in Paris in November, the US government got its mojo back on the subject of encryption after two years of being on the defensive about the subject.

Two years ago, of course, give or take a few months, Edward Snowden revealed to the world the extent to which the US government had access to, well, everything that was happening online.

The US then watched, somewhat helplessly and definitely very frustrated, as companies such as Apple and Google made encrypted-communications available to the masses. These vendors had to make clear that they were no one’s patsy — certainly not the US government's! — if they wanted to continue to do business with the rest of the world. Which they certainly did.

It Didn't Matter Anyway

As it turned out the steps US companies were taking to assure their global customers that the US government would not have access to their communications did not stave off the Court of Justice of the European Union's decision this fall to strike down the 15-year-old Safe Harbor Framework — a set of rules that allow US companies to import European personal data while complying with strict EU privacy regulations.

The US Government Strikes Back

Then came the carnage and the horror of the terrorist attacks in November and the US government's pushback on encryption was back on the menu. It couldn't do anything about the EU's stricter path on privacy but it could push for new legislative measures that it deemed necessary.

Congress had been holding hearings on encryption earlier this year, and tried to push forward a bill expanding the data sharing between the private sector and the government. It was blocked despite encouraging noises from the Obama Administration that it would sign the measure.

The bill was revived and slipped into the 2,000-page $1.1 trillion spending and tax bill passed this month by Congress to fund the government for the next fiscal period.

Called the Cybersecurity Information Sharing Act (CISA), it establishes that private companies may provide information to federal agencies law without fear of being sued. This information would relate to "cybersecurity purposes and responses to imminent threats or serious threats to a minor."

The crimes that the federal government can prosecute using this information include "fraud and identity theft, espionage, censorship, trade secrets, or an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or use of a weapon of mass destruction."

What's Wrong With That Picture?

In theory there is (unless one is a strict privacy advocate) nothing is wrong with these events -- and certainly none of this is meant to dismiss the deadly threat that is terrorism and the grim necessity of fighting it.

In reality though, the US government’s focus on encryption and other steps it has taken to gain control over the illicit and dangerous communications communication on the Internet have completely missed the point. (Unless, of course, one is a defense attorney concerned about the new warrantless search rights the government just carved out for itself. Or a Fourth Amendment advocate).

Or, let's put it this way. The US government just expended a lot of political capital to fight what is just a small battle in a much bigger and intricate and very global war. It also has just made the same mistake it repeatedly makes about technology -- trying to legislate for something that is constantly changing and morphing.

The thing is, businesses were always relatively safe from lawsuits in this issue, assuming their privacy policy didn't specifically state they wouldn't share information with the government which it almost surely did not.

And the government's obsession with keeping encryption under its control?

1) Encryption can be broken

2) There is no evidence that terrorist groups are using encryption to hide their communications and

3) advances in quantum computing are bringing us closer to the day when quantum-resistant algorithms will be able to breach even the most secure of cyber protections -- or evade them.

Ring-Fencing the Low Hanging Fruit

Meanwhile little heed its being taken of the low-hanging fruit still available to hackers. 2015's overarching online security narrative has been the regular security breaches of retailers and banks and insurance companies and even the federal government.

This is the stuff that drives online ad fraud, malvertising, hampers e-commerce, increases costs for businesses significantly (perhaps even more than their liability insurance?) and ultimately affects national security as well. That breach of the Office of Personnel Management? It swept up the files of people with very high security clearances.

And hackers have proven, like roaches, to be highly adaptive to measures taken to eradicate them. One theory about the rise of ransom-ware is that the growing use of ad blocking technology made malvertising too time consuming so they moved on.

Indeed, one security prediction for 2016 by the Irvine, Texas-based security researcher Trend Micro is that online extortion will be enhanced through the use of psychological analysis and social engineering of prospective victims. "Despite the growth in security investments and legislation, these changes will inevitably bring new, more sophisticated attack vectors," said Tom Kellermann, chief cybersecurity officer of Trend Micro.

What's Next?

So what can be done? Unfortunately, there is no easy answer and every now and then a survey coughs up a factoid that makes one despair about how online security can ever be guaranteed.

But for starters business and consumers need to get real about the dangers of a complaisant attitude to online security. It didn't happen this year. Maybe next? Here is one place to start. And here. And here and here. You get the picture.

Submitted by: Ruth Edge Cardinia Shire Council