**Business differentiation through cybersecurity**

November 14, 2017

Aleksandr Värä

Technical Services Sales Director

A picture containing invertebrate, jellyfish

Description automatically generated

A while back I was thinking of switching my old car to something modern and went to a car shop of one of the most advanced car makers. There I got a great speech about how connected cars deliver more value throughout the car ownership cycle by delivering constant updates that positively affect passenger safety, car performance and overall driving experience without the need for additional investments. I also learned that I could buy new functionalities for the car from the company’s website and those would be downloaded and installed in the car overnight, which means I wouldn’t have to make decisions on some of the additional car features in advance, prior to buying the car itself. The sales rep was even capable to calculate a good RoI, compared to my current gasoline-feasting, air-polluting, tree-eating monster.

As I was basically sold, which is not an easy accomplishment, a question popped into my mind; "if this car gets updates that may affect the car’s performance and safety functions via the internet, how can I be sure that the car can survive a potential hacking attempt, without threatening the passengers?" Suddenly the highest value that the sales rep was proposing (connectivity) became a huge red flag to me. Although the sales rep tried to fix the situation, statements like “we take security seriously” and “we have the capability to patch the car remotely”, do not really make me trust one’s products, especially safety-critical ones.

I'm positive that the car vendor in question takes cybersecurity seriously. At the same time, I was very surprised by how hard it was for the sales rep to leverage cybersecurity in terms of added value. After all, I can imagine that with media covering major cybersecurity/privacy incidents, it's only a matter of time when product security and privacy will affect consumer purchasing behavior in masses.

I’ve gathered some ideas and examples from the internet on how one can leverage cybersecurity investments to gain customer trust. Obviously, not all of them work for everyone, but perhaps you'll find something useful for your product positioning and differentiation. Feel free to explore and add more ideas of your own!

**Let your customers know that you take security seriously**

Of course, you have hired the best superstar security team or collaborating with a cybersecurity company to ensure that your products are secure today and tomorrow, so why not announce it?

**Be proactive**

Create a separate page on your website explaining in human-comprehensible language, how you are actually making sure that the bad hackers won’t get into your customers' products. Truthfully speaking, everyone knows that security can fail. By communicating your preparedness and potential measures to sustain or mitigate a cybersecurity breach, you will definitely show preparedness and concern for your customer’s security, safety and privacy.

**Publicly reward people who help you make your products safe**

There are a number of communities as well as individuals that are searching vulnerabilities in products during their free time or due to a higher calling. In addition to monetary rewards, give a shout-out to the public, thanking them for their efforts. Compete in different bug bounty events or establish your own. Don't be shy to utilize these events in your marketing. This way you'll ensure that in addition to your security team, you will get additional support from the "white-hat" community. Your customers on the other hand may experience more trust towards your brand, as they can tie it to product security.

**Innovate**

You know your products best, which enables you to create cybersecurity solutions specific to your products, not seen by the rest of the world. Promote your security innovations! Not only you will gain respect from your clients, those security superstars that I mentioned a few paragraphs back will be more interested in you as an employer, probably making your efforts of hiring them a bit better, as the competition for the best cybersecurity professionals is hard nowadays.

**The first step**

If you are a product owner or a marketing expert and like the ideas above or perhaps have some of your own, do not hesitate to establish a relationship with R&D and security organizations within your company. Although they seem to be working in their dungeons and are under a heavy workload, I’m pretty sure that they are willing to contribute to your efforts to add value for your customers through cybersecurity. The value is most probably already there, it’s just the communication link to the outside world that needs to be established.

**Some examples**

Why should you be trusted: [https://techcrunch.com/2017/03/14/apple-hires-security-researcher-jonathan-zdziarski/](https://techcrunch.com/2017/03/14/apple-hires-security-researcher-jonathan-zdziarski/" \t "_blank)

Proactive statement: [https://transparencyreport.google.com/](https://transparencyreport.google.com/" \t "_blank)

Public awards: [http://nordic.businessinsider.com/finnish-spare-time-bug-bounty-hunter-found-an-error-worth-a-$22000-reward-2016-10/](http://nordic.businessinsider.com/finnish-spare-time-bug-bounty-hunter-found-an-error-worth-a-$22000-reward-2016-10/" \t "_blank) , also the hall of fame idea is quite cool [https://www.tesla.com/fi\_FI/about/security](https://www.tesla.com/fi_FI/about/security" \t "_blank)

Innovation: [http://drives.danfoss.com/newsstories/drives/industrial-iot-innovation-receives-international-recognition/?ref=17179934118#](http://drives.danfoss.com/newsstories/drives/industrial-iot-innovation-receives-international-recognition/?ref=17179934118" \l "/" \t "_blank)

**Source:** **https://www.linkedin.com/pulse/differentiation-through-cybersecurity-aleksandr-vara/**