

## All.Net Analyst Report and Newsletter

### Welcome to our Analyst Report and Newsletter

#### 20 Reasons Russia will Never Defeat our All.Net Security

Just kidding – but I thought it would get your attention.

- **Russian attackers – if you are reading this, I'm sorry – I didn't mean it!!!**

So many cybersecurity companies over the years have claimed 100% protection and similar things that I wanted to make sure you don't believe any of them. They are either ignorant, lying, or true believers with too much faith in themselves.

So I thought I would list the (first) 20 reasons (excuses) for not doing anything about your security. Believe me when I tell you I have heard these rationalizations from actual CISOs, CIOs, and CEOs.

- **Reason 1: We just asked them politely not to do it.**
  - Hopefully that will counter the ridiculous brag I started with. To quote from the old western saying I quoted in my dissertation:  
*"Ain't a horse that can't be rode, Ain't a man that can't be throwed"*.
- **Reason 2: The power of prayer**
  - OK – this seems unlikely to work, but please feel free to try it.
- **Reason 3: We have a new and unique approach that they will never get around.**
  - No you don't. You are just fooling yourself.
- **Reason 4: The NSA trusts us (but from that company)**
  - The NSA just adopted a Zero Trust model – so they don't trust you – and even if they did, I don't trust them... to protect the rest of us... when they cannot even protect themselves.
- **Reason 5: We are part of the Zero Trust Alliance!**
  - I don't know if there is such a thing, but even if there is, I don't think it will help.
- **Reason 6: There is nothing to ransom**
  - They will find something you value if they want to get you.
- **Reason 7: We don't have anything for them to take!**
  - Only your life and everything you own. And yet they might try.
- **Reason 8: Our security is so complex nobody could ever figure it out.**
  - I think you mean it's so complicated you don't understand it. But complexity is the enemy of security, and complexity doesn't defeat serious attackers.
- **Reason 9: You're just being paranoid!**
  - You're not paranoid if they are actually out to get you. And they are...

- **Reason 10: I use XXX cloud services.**
  - All of the cloud service providers are susceptible and most have been attacked successfully in the past.
- **Reason 11: I have cyber-insurance.**
  - In almost all cases, not worth the cost of making the claim. And if it is, the insurers are starting to lose their shirts in this arena.
- **Reason 12: They have never gotten me yet...**
  - As far as you are aware... And even if true, they are not done going through the list.
- **Reason 13: I'm too small for them to bother with.**
  - They even go after individuals and small businesses.
- **Reason 14: I'm too big for them to dare.**
  - So you are bigger than the US Government?
- **Reason 15: I don't use computers.**
  - Then how are you reading this?
- **Reason 16: We have a great team and I am confident in them.**
  - Don't be ridiculous. The best teams have lost and won in different encounters. And no matter how good your team is, you are fighting against a team with far greater resources and access.
- **Reason 17: We run Linux so we are safe.**
  - No operating system vendor can make you safe.
- **Reason 18: We run OSX so we are safe.**
  - See Reason 17.
- **Reason 19: We run (name your operating environment) so we are safe.**
  - See Reason 18.
- **Reason 20: We trust our people!**
  - The Russians will still get in, by a combination of technical and non-technical means.

### What to do about it?

“My dog's better than your dog, my dog's better than yours...” [Kennel Ration commercial]

Stop imagining that you will be able to win every time and start working on how to do better on a statistical basis by managing risks. And stop buying into vendor claims. Security is something you do, not something you buy. You should only buy things to help you do it well.

Start by doing governance well. This is not a “technical problem”. It cannot be solved by technologists. It is a governance problem that can only be solved by executives making good decisions and controlling their companies to carry those decisions out.