**The Biggest Issue in Cybersecurity is Humans, Not Machine**

Rachel Botsman

Wired Security

ITA 120

Professor Natalia Emicioi

September 17, 2021

**Abstract**

The video title *The Biggest Issue in Cybersecurity is Humans, Not Machine* is conducted by Rachel Botsman who is the author of *Who Can You Trust?* It dives into how the root of cyber and tech errors are usually because of human error and more specifically trust. Ms. Botsman starts the conversation talking about trust signals and how they mislead people into trusting apps and companies without having the full information. From there the discussion goes to how money and trust are intertwined when it comes to cybersecurity and how misinformation can lead to all sorts of issues. Another great point that is touched upon in the latter half of the speech is the evolution of trust and access in online companies and how it went from local to now distributed trust and info. All in all Rachel Botsman informs the people that not only is trust a two way street but that more times than other it is the trust and amount of trust we give that lead to cybersecurity issues.

KeyWords: Money = Transaction while Trust = Interaction, “Efficiency is the enemy of trust”

Evolution of Cyber Trust = Local institutional Distributed. Trust, Cybersecurity, Proactive, Reactive, trust signals.

**The Biggest Issue in Cybersecurity is Humans, Not Machine**

**Introduction**

In Rachel Botsmans speech about the biggest issue in cybersecurity being humans and not the machine, she starts off by introducing trust signals and what they mean. She also talks about how at times these signals may be misleading of the person. This same idea is then correlated to how problems in the cyber worlds tend to start from the trust aspect companies have with their users. This is a direct result in modern technology and online companies offering on demand services. This not only leads to faster goods and services being provided, but also the users having to share more information than usual with these sites.

**Literature Review 1.1:**

Alix Paultre in his article, “Establishing Trust in Cybersecurity touches upon a similar point on how this on demand service is now leading to all avenues that hackers can hack your system and steal information. He goes on to sit down with the Vice President Alan Garu of Embedded Solutions, and he goes on to explain how installing cybersecurity into devices is a must before it enters the shelf. He then states, “In his opinion, every and any device needs to have some type of secure boot to keep the device secure if there are hardware ramifications with the device. (Paultre, 2020). The author Alex then goes on to speak about how blockchain and multi-step authentication is another great way to prevent cyber hackers and build another wall of defense.  The issue of cyber-attacks is prevalent in many ways and can come from wireless sensor networks as well. Although this is more of a simpler issue, there are still some minor problems in combating cybersecurity when it comes to wireless network like energy sources.  “Undoubtedly, the failure of the sensor nodes is generally due to the exhaustion of their batteries”, says Djallel Eddine Boubiche (D. E. Boubiche et al 2020).

**Literature Review 1.2:**

The cybersecurity risks in CPS(Cyber-Physical System)have increased rapidly in the past decade .Also, CPS has been increasingly deployed in critical infrastructure, manufacturing and everyday life such as building control, medical devices and smart grid (. Walker-Roberts et al 2019). Steven Walker‑Roberts, who is one of the authors, states that the majority of cybersecurity incidents are often coupled with the added caveat and vulnerabilities that are discovered and are either kept secret or are only shared within technical circles ( Walker-Roberts et al 2019). She goes on to explain that this is possible because there are huge datasets that are shared and compromise cybersecurity. This final article that I found titled: *Threats on the Horizon* closes off one of the sections by letting us know that many devices don’t get enough security updates and that this is practically due to the fact that CPS devices are managed by operational tech teams rather than IT.

**Reflection 2.1:**

It’s becoming obvious that cybersecurity attacks are getting more and more complex and coming from all different angles and strategies. One common factor that I am recognizing here is that human error is very prevalent and may also be the main cause of cyber-attacks. Not only are there mistakes made in operational teams and large professional cyber teams, but we also see it at the lowest level with users not updating devices or adding Secure Boot and other software’s to help from attackers. This level of ignorance is a key factor in online companies getting your trust and you being hacked. The distribution of information through online apps is something that is growing every day and your information is being passed around. It is on the human to take control and put in the necessary parameters needed to keep yourself protected.

**Reflection 2.2:**

Online companies and networks pick up your information in multiple ways like through authentication and Terms of Service which many usually don't read. Personally, I agree with Rachel Botsman in her assessment that cybersecurity issues come from misjudgment of the human being and who they are giving their trust too. I say that because with trust comes access and that’s all that's needed for cybersecurity attacks to start. The best way to get ahead of the situation is to add security to your device beforehand. This not only gets ahead of the problems but also doesn’t leave space for human error that you would make. The threat of attacks has become greater as technology evolves. We see now with distributed trust it’s harder to not share data or info with all these social applications popping up. From there it is up to the company whether they will be proactive or reactive to the issue and take action.

**Conclusion 3:**

In conclusion we see that modern technology and computers aren't the biggest problem, and that it most likely can be from misinterpretation of trust signals from companies and peoples. This not only leads to humans giving information that they shouldn't be sharing and online companies distributing that info around the internet for hackers and cyberattacks to get. We must also remember that trust has been modified and evolved with the industrial revolution leading to corporations and companies getting bigger and diving into more of a business trust than a local trust circle. The author Rachel Botsman claims that this evolution of trust is the problem and does not work in this digital age because it is not moving in a normal hierarchy where it goes up to authority and regulators, but instead spreading through networks and marketplaces where the risk of cyberattacks are very high. With money transactions and paypal it becoming easier for cyberattacks to get sensitive information from just outsourcing to different websites you visited. This is the risk and reward of digital evolution that is an ongoing battle in cybersecurity and is still being fought till this day.

**Visual Aid:**



Figure 1



Figure 2

[Figure 1 6](#_Toc82810444)

[Figure 2 6](#_Toc82810445)

**References/Citation**

(Steven Walker‑Roberts1, 2019)

(Djallel Eddine Boubiche, 2020)

(Paultre, 2020)

# Bibliography

Djallel Eddine Boubiche, S. A.‑C. (2020). Cybersecurity Issues in Wireless Sensor Networks: Current. *Wireless Personal Communications*, 38.

Paultre, A. (2020). ESTABLISHING TRUSTIN CYBERSECURITY FOR EMBEDDED SYSTEMS. *Evaluation Engineering*, 5.

Steven Walker‑Roberts1, M. H. (2019). Threats on the horizon: understanding security threats. *The Journal of Supercomputing* , 23.