Cybersecurity – Accept Fear of Danger, Harm, and Threats?

Erland Wittkoetter, Ph.D., Aug 29th 2022

Security is on the side of potential victims. Moreover, security or safety usually gives us freedom from fear of danger, harm, or threats, including protection against problems intentionally or accidentally caused by others. Most security is hidden or only discussed by professionals and experts quietly. If security is mentioned, then because involved peoples are proud of it, or we are reminded not to do something non-common-sensical. In all other situations, when security is mentioned, it should make us aware of (serious) security-related problems relevant to our decisions or being prepared or alerted against preventable damages.

Generally, security protects us from damage in uncertain or malicious environments. It defends us from adversarial attackers intending to harm us. Product liability or regulation is based on extensive technical expertise; it has prevented a lot of harm. Security and product safety measures have made fatal failures rare. Security technologies and measures are usually confident in their delivery. They know they must accept the consequences of failures. Someone is always responsible if product safety fails. Food, drug, aviation, or nuclear safety agrees on tough regulations with penalties when failures happen; this is good for their business. Even home security systems have satisfied customers giving (positive) feedback after incidences.

Cybersecurity seems an outlier in some of their delivery. Frankly, we should expect performance with similar rigor and demand for reliable results. Instead, many pros in cybersecurity seem to be demoralized. Public trust or expectations in cybersecurity is already low. Blaming others is the name of the game. Product certifications are unlikely sufficient, but they are better than nothing. Audited/certified products confirm that buyers' decisions are not to blame. Vulnerabilities undermining security are found eventually. Full audits are too complex and likely insufficient anyway. The shared distrust in cybersecurity measures and fear of incalculable damages from security breaches is justified. It is not hard to imagine becoming the next victim. It is as if we already accept the fear of (possible, long-term) consequences and damages. Promising in this situation peace of mind would likely be considered deceptive marketing. This situation can only be different if cybersecurity gets proactive, preventative, and redundant, i.e., if it delivers security as in other tech sectors.

With malware and trojans around us, internet security based on encryption, i.e., SSL/TLS, is unfortunately not good enough. Attackers know what they deal with and want: access to session keys – or, more explicitly, covertly, tracelessly stolen crypto-key for manipulating eCommerce transactions. At least a 2-Factor-Authorization (2FA) is required. Unfortunately, this patch is temporary; it does not solve the underlying trust problem.

It seems human nature to blame others or technology for their own mistakes. In users' perception, stories of super-capable AI in the hand of criminals could soon make the news. Even unproven rumors could become accepted mainstream opinions. Then people will use criminal AI as an excuse and reason for their misfortune or mistakes. Who will carry the burden of proof if this becomes a legal matter? Damage seems to be inevitable.

Cybercrime is labor-intensive, but criminals have access to resources allowing them to use artificial intelligence to simplify their tasks significantly and potentially use enhanced cyber capabilities with profit. There are already an estimated 1 trillion dollars in damage annually from cybercrime; much of it is based on deception and dishonesty. But once public trust in e-commerce takes a significant hit, damage will be even more catastrophic. This situation is unacceptable. **Cybersecurity must become proactive and preventative (asap)** and establish (irrefutable) trust in its solutions. Unfortunately, cybercrime will not vanish, but its damage should not be caused by malware. At a minimum, we must eliminate malware, ransomware (data sabotaging), spyware, and backdoors. As a result, we could regain trust in encryption (at least among professionals) and its application in eCommerce, online banking, and logistics. **These goals should be non-negotiable**.

Cybersecurity should guide/help/protect people with their inherent (often unavoidable) vulnerabilities and how they can be protected from being scammed; it should not get involved operationally in tasks that can be fully automated. Having humans involved in low-level security makes it only less reliable and trustworthy.

As the first goal of cybersecurity, we should end nation states' ability to conduct cyberwars, which is doable quickly (e.g., via hooksafe-type solutions). The goal should be to stop cyber-warfare through an open-sourced grassroots development project that should also facilitate the defense against more capable cyber adversaries.

More info: https://NoGoStar.com

 info@NoGoStar.com