For 2023, Here Are Five Hopes For Cybersecurity

The 2023 Cyber Wish List

The Leaders at **eos**edge Legal and OnCall Cyber™, after observing the changing cyber and crypto landscapes over the past year and beyond, offer these beliefs and recommendations for improving cybersecurity for 2023.

Views about cybersecurity from cyberlaw professionals:

1) **Pass laws that install property ownership rights to proprietary and identity data**
   The Basic Idea: Data is property after all, though defining how individuals and entities own their data under property law would create an incentive and a more efficient enforcement atmosphere for infringed owners to redress harms. The current privacy-based construct is inefficient and difficult to enforce – as in: what exactly is the cost of a loss of privacy? In particular, Web3 technology is already architecturally enabling data ownership, but the law needs to keep up.

2) **Pass laws that create a government backstop for cyber insurance**
   The Basic Idea: Insuring cyber risk has proven to be difficult to define, and so insurance carriers have been raising premiums, excluding types of attacks, and even exiting the market. Yet, insurance is needed for the market. So, like terrorism insurance models in certain countries, the government should step in to cover catastrophic risk. In turn, this backstop would restore availability and affordability to the insurance market.

3) **Pass laws that empower data collectives and trusts**
   The Basic Idea: Adding to #1 – Data Ownership – the ability to enforce property ownership rights must become universal and affordable. Less financially secure individuals, through legal mechanisms created to pool and protect collective interests (aka a Data Trust), efforts to enforce rights against data ownership infringements would become affordable. Moreover, with efficient and universal enforcement mechanisms, deterrence against cyberattack becomes real.

4) **Pass laws that compensate victims of cybercrime**
   The Basic Idea: Certain laws, such as in the US – United States Victims of State Sponsored Terrorism Fund (USVSST Fund) – provide a way for governments to seize assets from entities determined to have been involved in supporting terrorism. In turn, victims can pursue financial claims through the courts against those frozen assets. That is an excellent construct to adopt against cyberattacks because so many advanced hackers have connections or tacit permission from rogue states.

5) Require a Cyber Expert on every Board of Directors

The Basic Idea: Cyber Risk, as the cyber insurance industry has learned, presents a problem set which most corporate boards cannot readily appreciate. As a result, budgets, priority, brand protection, and even reasonable decision-making goes lacking in steering the business. Corporate boards need to better understand the duties, the risks, and the liability exposures from cyber risk which must be addressed to properly run a business nowadays. Leadership comes from the top, and corporations all need cyber expertise on their Boards of Directors.

The Details

The reader should note that these Wish List Items are all cyberlaw innovations. Fixing cybersecurity from a structural and strategic point of view requires the institution of law. Afterall, cyberspace has become a globally destabilizing proposition. Hence, changes in structure necessitate changes in law.

Passing Laws that Install Property Ownership Rights to Proprietary and Identity Data

If a framed photograph is indisputably a piece of property and its theft redressable under both criminal law and property law, why is online identity theft enforced under privacy law? Why is a digital image treated differently than the framed photograph? And to take that logic further, why aren't all vestiges of identity and all aspects of one's digital identity information treated under the law as one's property?

Data-as-property is the vision and enablement afforded from the decentralized nature of Web3. However, the legal construct which has been created worldwide to date which surrounds data is a privacy construct (e.g., GDPR in Europe). Enforcement of GDPR and all privacy laws and regulations, however, does not scale. And proving privacy harm is difficult. Conversely, property law – both common law principles and intellectual property statutes – is a far more efficient and effective body of law for protection and enforcement actions.

Moreover, online harms are multiplying, metastasizing and mutating. Deep fakes, disinformation, counterfeit nonfungible tokens (NFT), and similar threats emerging from technological innovations stand to disrupt global society. The law must step in to restore order. Clear ownership rights to data, both identity data and other intangible data (e.g., corporate goodwill), could enable property-based infringement actions to be pursued against misuse or unlicensed use.

Put simply, data ownership – all the rage in the Web3/crypto space – is actually a game-changer for cybersecurity!!! Laws must be passed to clarify data ownership rights under property law.

Passing Laws that Create a Government Backstop for Cyber Insurance

At the end of 2022, the CEO of Zurich Insurance, Marco Greco stated that cyberattacks were destined to become "uninsurable". Having an uninsurable risk from cyberspace is untenable for business. There are mixed views within the insurance industry regarding its desire for a government role, but catastrophic risk has often become the impetus for government to step in.

A law in the US, Terrorism Risk Insurance Act (TRIA), is an example and a potential model to adopt for the cyber insurance market. Like terrorism, cyberattack can be a catastrophic risk. Increasingly, the

ransomware attack scourge is shutting down hospitals, power and energy facilities, and entire cities! Moreover, the Saudi Aramco and Sony attacks – both attributed to state actors – prove the point that private companies should not have to face the financial costs of recovering from a sophisticated state actor-affiliated attack. Hence, a role for government, even in the insurance market, exists for cyberattacks.

Passing Laws that Empower Data Collectives and Trusts

Along with passing data ownership laws, accompanying legislation should enable other ways that data should be managed as an asset class. First, from a cybersecurity national strategy perspective, creating an incentive for the universal interest in protecting one's digital property would create deterrence against cyberattacks. In other words, just like people and all of society do not stand for having their money stolen, a system of enforcement would spring up if data ownership rights were enhanced through the ubiquitous use of data trusts.

The notion of a data trust, or a collective or pooling of data among individuals or entities with certain shared interests, would facilitate a cost sharing for rights enforcement. Collectivizing or pooling of interests and rights is a common tactic for gaining leverage – think unions, collective bargaining instruments and similar collectives. Because real deterrence cannot have very many gaps for the cyberattackers to exploit, mechanisms are needed to create universal data rights protection. Laws that treat digital identity and digital asset classes as property and establish incentives and protections for data trusts would bolster a strategy of combating cyberattacks through a multi-faceted data-as-property legal framework.

Passing Laws that Compensate Victims of Cybercrime

Like the ideas above, deterrence is aided by enforcement schemes which remove the incentives of cybercrime. Moreover, an effective deterrence strategy for cyberspace requires both public and private sector actions. What the USVSST Fund model demonstrates is that, along with government sanctions and asset seizures, private parties can petition the courts for financial compensation. The result is that the fruits of crime, the financial incentive, is diluted when monies can be returned to victims.

Investigations have shown – from law enforcement, investigative journalism, and other private sector mechanisms – that certain crypto markets, gray markets, and other IT networks – have been used for cybercrime. Along with the data-as-property legal framework noted above, property-based legal theories can be more efficiently used to recover stolen assets. For example, contributory infringement claims can be pursued for copyright, trademark and patent violations against the indirect violators. There will undoubtedly be collateral damage under this theory, just like botnet takedowns harmed innocent third parties. However, the interconnectedness of cyberspace seemingly requires improved know-your-customer practices, and that would mitigate the collateral damage concern.

A trustworthy Internet is an imperative for commerce. Deterrence of cyberattacks must be improved. Seizing assets used in cybercrime, and in turn creating compensation methods for victims of cybercrime that can recover from seized assets looks like an attractive model that would aid deterrence.

Requiring a Cyber Expert on Every Board of Directors

This one seems like a no-brainer. It is not a new idea; however, its adoption is not uniform. It is odd that there is a dire gap in the workforce around the world for cybersecurity staff, yet at the Corporate Board level there is hardly any movement or appetite for cyber leadership.

Less, rather than more, needs to be said about requiring every Board of Directors to appoint a cyber expert. The need speaks for itself.

eosedge Legal is the trusted partner to the IR Global membership for cyberlaw and security services. OnCall Cyber™ is its trending venture to offer a Cyber Crisis Team subscription to help companies become cyber ready.