Shifting Values and Valuables

Summary: Technological, generational, and economic changes are reshaping ideas about what is valuable. In particular, information—especially in digital forms—is becoming more central to corporate functions and peoples' lives. Organizations will have to navigate diverging views of risk, of what is valued, and security will have to continually adjust to what is seen as worth protecting.

Forecasts

- Technological and generational trends will continue to shift markets away from physical products and toward services, access, and digital information.
- Companies and governments trying to serve a diverse and polarized population will find wide divergence in what their customers value, as different "tribes" ascribe worth to things others don't care about or even object to, e.g., the trade-off between security and privacy.
- In an information-driven world, reputation will continue to increase in value for organizations and consumers. It will be crucial for access—for organizations, access to consumers and their attention; for consumers, to services of all kinds.
- Misalignment between what companies value and what their workforces value will grow as outsourcing and the gig economy expand, creating issues of loyalty and security.
- Corporate value will shift further into networks, information access, and algorithms, rather than physical assets and production. The security and integrity of artificial intelligence software will be increasingly crucial.

Key uncertainties affecting what is valued:

- Changing economic conditions
- Degree and nature of cybercrime and cyberwarfare
- Evolving balance of offense vs. defense in cybersecurity
- Levels of stability, in key markets and internationally
- Effects of social and political polarization in different societies
- Speed and extent of move away from ownership toward rental and access
- Size and nature of generational value shifts and their effect on what is valued

Supporting trends

Data-trail control. People are generating vast data trails of personal information, leading to growing questions about who should own and control that data**.**

Fears of technology. Polling finds people fearful of a variety of technological developments, including cyberterrorism, pollution, identity theft, biological warfare, and corporate and government tracking of personal data.

Millennials now the largest US generation. Millennials have surpassed Boomers in numbers.

Concern about online privacy. Polling finds that consumers are very worried about the privacy of their personal data online.

Millennials more proactive about online privacy. Younger adults are more savvy and proactive about protecting their privacy.

Growing middle classes in emerging markets. The world's middle classes continue to grow.

Growing freelance workforce. More than one-third of the US workforce was freelancing in 2016.

Sharing economy growth. The sharing economy is forecast to continue its growth.

Consumers like encryption. Strong consumer trust in encryption will continue to make it difficult for law enforcement and government to build back doors into systems for security purposes.

Genetic surveillance. The potential for intrusions on genetic privacy are growing.

Who owns the DNA? Courts are beginning to sort out the question of who owns a person's DNA.

Data points

What is your data worth? People believe their new digital possession have worth, but differ on the details. A survey found that the average U.S. consumer believes his data to be worth around $4,500. This number differs between men and women, with men valuing it at $5,874, while women offer a lower estimate of $4,375.

Valuable = stealable. New forms of valuables are subject to theft. For instance, the cybersecurity company Darktrace reports that incidents of illicit use of computers to mine cryptocurrencies climbed to hundreds per month in 2017, with an estimated 25% perpetrated by employee insiders at firms.

Topics for additional research

- Gaps between what companies and consumers now value and how well they are protected
- How generational and demographic groups differ on what is valuable
- How privacy and its protection are evolving

Strategic insights

For the security industry

- Organizations will need new forms of risk assessment and cost evaluation in order to understand what needs to be protected and how. Widening gaps between what is or is not protected and at what level are areas in which to hone the value of security functions.
- New valuables create new opportunities: for example, the protection, recovery and reconstitution of digital products will be an increasingly lucrative business, and insurance companies are protecting virtual possessions; for instance, some now sell policies covering injuries affecting fantasy football leagues.
- There will be a diversification of what is considered valuable by people and societies, in domestic markets and internationally as global middle classes continue to grow. This will create more niche security functions and markets in the industry.
- To understand and protect new conceptions of valuables, the security industry will need to broaden its definition of security professionals and their skill sets, and have a wide range of generational, cultural, and socioeconomic diversity.
- Marketing security products and services will grow more fraught in polarized and divided societies. Trends that evoke fear and revulsion in one group may be embraced by another. Very different marketing approaches may be needed, even for the same services.

For ASIS

- ASIS could position itself to help the industry navigate issues in providing security across borders with training and guidance; especially in online issues, jurisdictions are putting forth rules and laws that may conflict with the laws and norms of other countries.
- As with many societal changes there will be an institutional lag (e.g., in law and insurance) in adapting to the new landscape. ASIS could have a role in sorting through emerging issues in value and its protection and creating new institutional approaches.

Timing

- **Stage**: Growth, with active driving forces
- **Speed**: Rapid, driven by technological and social change

Potential alternative futures

- **Values amidst fear**: War or high levels of terrorism cause more societies to concentrate on the most basic concerns and values.
- **"Digital Sept. 11th"**: A truly disruptive digital breach or cyber attack shocks the public and politicians and forces wholly new approaches to the Internet and cybersecurity.
- **Taking back control**: Companies are forced to respond to a widespread consumer need to feel more in control of one's life and possessions that spurs interest in physical goods, defined ownership, and restricting outside access to data**.**
- **Balkanized security**: Security services and functions are divided in the face of growing societal polarization and low trust.