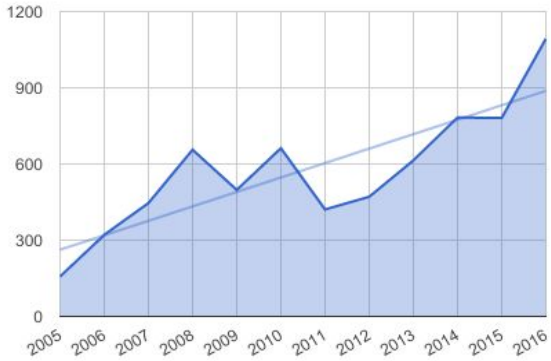
Summary

The Internet and related technologies give us unprecedented access to information and each other that consumers—most of us—would like to enjoy our lives online without worry. In the real world, however, we seem to be increasingly waiting for the other shoe to drop. Not only can we be attacked at home, but data breaches like those suffered by Equifax and Target put our information, even our identity, at risk. As a matter of fact, over 64% of US consumers have "personally experienced a major data breach" as of 2016.[1] Moreover, this has not been getting better: data breaches have been trending upward since 2005 (see Figure 1).

A troubling fact is that the upward trend comes despite the promulgation of myriad laws and regulations to protect consumers digital rights and privacy, including PCI, HIPAA, and COPPA. It has also been more than a decade since the TJX breach hit the headlines and put data security on the map. The trend continues despite climbing spending on cybersecurity by government and large businesses (see Figure 2).

Does this mean that consumer's information will never be secure? Many people believe it can't be. They believe it pointless to try. While security can never be total in the digital world, as in the physical world, there is much that can be done.

Figure 1 Number of Data Breaches Since 2005



Source: Identity Theft Resource Center http://www.idtheftcenter.org

[1] Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," http://www.pewinternet.org/2017/01/26/americans-and-cybersecurity, (January 26, 2017).

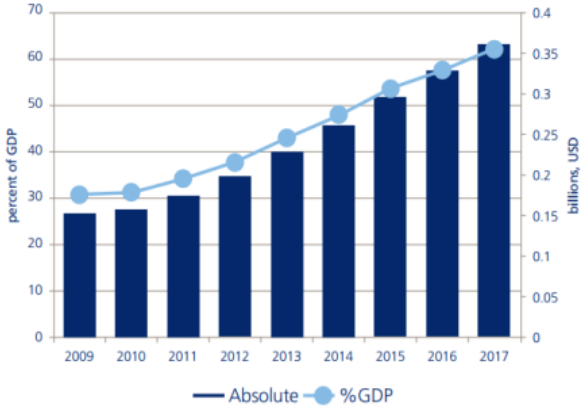
Challenges for Consumers

The Internet and other parts of the cyber world seem to be ever more hostile, filled with scammers, thieves, and competing nation states, all exploiting weaknesses in the digital universe. They confront consumers—ordinary people—with two sets of challenges.

Protecting the Home

First, consumers need to protect their homes. Once upon a time this meant protecting information. But with the ever-spreading Internet of Things it increasingly means protecting the home from attacks that at one time could only be done physically.

Figure 2 Cybersecurity Spending in the US, Percentage of GDP (in Billions)



Source: Risk Nexus- Overcome by cyber risks? Economic benefits and costs of alternate cyber futures, available at http://publications.atlanticcouncil.org/

Moreover, the criminally inclined have continued to find new ways to bilk their victims. Older methods, like ransomware, have been dressed in new tech, like the Wannacry virus. And the Internet of Things is generating new targets. Much of the Mirai botnet, for example, is composed of devices like cameras found online.[2]. Mirai brought down a large portion of the Internet in 2016.

Medical devices pose a special new risk. An increasing number of them are being connected to the Internet. Many are vulnerable. Indeed, the FDA recently recalled almost half a million pacemakers out of concern that they could be hacked.[3] Most of the companies that make the devices and provide them to patients recognize the danger, but less than 20 percent of them are taking steps to prevent attacks.[4]

The market for devices and software to protect the consumer at home is large and growing. There is no absence of choice for the consumer, but the opportunity for fraudulent claims and simple fraud has grown to match the growth of their concern. Moreover, most of the vendors creating the new devices that make up the Internet of Things treat security as an afterthought, if they consider it at all, thus leaving consumers—and everyone else—increasingly open to attack. As cars and medical devices come online, too often with little concern for security,

Protecting People's Data

The other challenge that consumers face is that the data they own but organizations hold is vulnerable. The recent breach of Equifax is but the most recent example of this. The Equifax breach showed how consumers are rendered deaf, dumb, and blind when it comes to the protection of their sensitive information. The number of data breaches has risen steadily since 2005, and the Equifax breach isn't the biggest we have seen, but it may be the most damaging, exposing the social security numbers, drivers' license numbers, birth dates, addresses, and credit card numbers for up to 143 million people, 44% of the US population. Their response, was insufficient and, to be charitable, tone-deaf.[5]

---

[2] Symantec, "Mirai: what you need to know about the botnet behind recent major DDoS attacks" https://www.symantec.com/connect/blogs/mirai-what-you-need-know-about-botnet-behind-recent-major-ddos-attacks (October 27, 2016).
[3] U.S. Food and Drug Administration, "Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication" https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (August 29, 2017).
[4] Ponemon Institute, *Medical Device Security: An Industry Under Attack and Unprepared to Defend*, May 2017.
[5] Brian Krebs, "Equifax Breach Response Turns Dumpster Fire," https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/ (September 12, 2017); Davia Temin, "Equifax: A Category 5 Cybersecurity Crisis Storm. Chances Are It Will Hit You." https://www.forbes.com/sites/daviatemin/2017/09/09/equifax-a-category-5-cybersecurity-crisis-storm/#62dbaced71ee (September 9 2017).

Equifax and the other companies that hold consumers' data behave as if they own it. They shouldn't. They should regard themselves as custodians instead. It took Equifax two months after the breach was discovered to own up to the loss of the data. That loss occurred because a patch available two months before the breach occurred had not been applied. Similarly, after Wendy's was attacked in 2016, consumers continued to be compromised and defrauded for six months while the restaurant chain conducted its investigations.[6] Moreover, the breach was not made public by Wendy's, but by an independent journalist.

Financial institutions are not the only ones who fail as custodians of consumers' data. Medical records face even graver risks. One report found that nearly two-thirds of healthcare organizations and their business affiliates do not offer any protection services for patients whose information is stolen.[7]

Some people think that consumers simply do not care about data breaches. It is simply not true. One survey shows that more than 80 percent of the consumers interviewed expressed concern about the safety of their data.[8] Ponemon research shows that victim companies lost up to a 7 percent of their customer while 31 percent of consumers have discontinued a relationship with an organization that experienced a data breach.[9] Other research found that 76 percent of people would likely take their business elsewhere due to negligent data handling practices and that 71 percent would think twice about shopping at a retail store that had been hacked .[10]

Meeting These Challenges

Securing people's homes and data from the all too prevalent threats in the digital universe is not a hopeless task. People can be educated and empowered to do much of it themselves. And the institutions that consumers rely on to protect them and their data can take up their responsibility and become accountable for the digital protection of their customers and their data.

Consumers certainly need to be educated about how to protect themselves. Most simply don't know how.[11] Information is plentiful, but often not well publicized. It can often seem too complex for ordinary mortals. Just as smoking has been reduced over the years as its dangers have become better known, partly through wide publicity, publicity can make good practice in the cyber world better known.

The products and services need to have three characteristics in order to empower consumers. That they should be affordable should go without saying.

They should also be transparent. Companies that hold consumers' data need to be transparent about what data they hold, how they use it, and how they protect it. It is telling that Equifax did not collect data directly from the consumers whose data they lost. These companies also need to be open about when they fail, as many will.

---

[6] Brian Krebs, "There's the Beef: Wendy's Breach Numbers About to Get Much Meatier," https://krebsonsecurity.com/2016/06/theres-the-beef-wendys-breach-numbers-about-to-get-much-meatier/, (June 9, 2016).
[7] Herb Weisbaum, "Health Industry Can't Protect Your Records from Hackers: Report," https://www.nbcnews.com/tech/security/health-industry-cant-protect-your-records-hackers-report-n355401, (July 2014).
[8] Identity Theft Resource Center "The Need for "Secure Payment Agent" (SPA)," http://www.idtheftcenter.org/ITRC-Surveys-Studies/consumer-awareness-survey, (September 11, 2017).
[9] Ponemon Institute, *The Impact of Data Breaches on Reputation & Share Value: A Study of U.S. Marketers, IT Practitioners and Consumers*, May 2017.
[10] "Report Reveals How Cyberattacks Affect Consumer Brand Trust," http://www.securitymagazine.com/articles/87115-report-reveals-how-cyberattacks-affect-consumer-brand-trust, (May 12, 2016); Arbor Networks, "New Consumer Survey Shows High Anxiety about Online Security Does Not Translate into Action," https://www.arbornetworks.com/new-consumer-survey-shows-high-anxiety-about-online-security-does-not-translate-into-action (October 25, 2016)
[11] Kenneth Olmstead and Aaron Smith, "What the Public Knows About Cybersecurity," http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity, (March 22, 2017).

Transparency about the capabilities of products is also needed. For example, the installation of patches and updates for any application designed for home use should be effortless, but the consumer will need to know whether their systems are up to date.

Lastly, consumers need to find these digital products and services trustworthy. Transparency and a good track record over time will do much to create trust.

The wide adoption of products and services that have these characteristics will encourage cybersecurity best practices by increasing the accountability of those who provide them, which ultimately builds up a sustainable cybersecurity ecosystem for all.

The industries that have created the digital universe have done little to accept the flaws in the products and services they provide and to become accountable for their failures. Every software product includes an agreement that the company is not responsible for flaws in the product, yet few firms create them with security in mind. It will take a change in law, but the negligence that is common in these industries needs to change. Firms that collect consumers data need to be held liable when they fail as custodians; firms that cannot create products or services that meet basic standards for security need to pay the penalty when they don't.

Conclusion

In an increasingly digitized world, knowledge about cybersecurity is as critical as knowledge about physical security, if not more. As the number of people who rely on the Internet grows, so does the need to empower all users. Consumers need to be able to raise their voices if we are to build a sustainable and more secure cyberspace.

About Adaptable Security ----------

Adaptable Security Corporation (Ada for short) is changing the cybersecurity landscape by affording the individual users and organizations with a voice to protect their information and the power to choose whom to trust.

