JULY 2021

The Future of Digital Trust

A Research Project Conducted by the Aretiico TeamWork Collaborative

Annika AJAY	*Cornell University*
Gautam GOPINATHAN	*University of Warwick*
Zeyang LI	*Shanghai Jiaotong University*
Zoe SAVAGE	*University of Warwick*
Mollie SHEPTENKO	*University of Toronto*
Adrian YAN	*University of Warwick*

Table of Contents

Introduction

Sony's director of Information Security once famously said "I will not invest $10 million to avoid a possible $1 million loss," during an interview with CIO magazine in 2007 despite multiple warnings from various auditors (Holmes, 2007). About 7 years later, Sony Pictures Entertainment fell victim to hackers, who managed to leak very confidential data, including information about Sony's employees, plans for Sony films and more (VanDerWerff & B. Lee, 2015).

Fortunately, most companies and their leadership have changed their outlook towards cyber security, with spending on information security and risk management forecasted to reach $150.4 billion in 2021 (Gartner, 2021). In a survey conducted by Gartner in 2021, cyber security was found to be the "top priority for new spending," with "61% of the more than 2,000 CIOs surveyed increasing investment in cyber/information security" (Gartner, 2021).

It is, therefore, evident that cyber security plays a very significant role in most organizations.

A more accurate view on the importance of cyber security can be established by taking a look at the history of cyber security and what has been tried in the past, be it successfully or unsuccessfully. Some of the issues and conundrums of cyber security will also be discussed in this white paper.

Figure 1: Cyber Security Statistics 2020 (Swiss Cyber Forum 2020)

A Timeline of Cybersecurity (Avast Blog, 2020)

Cybersecurity has been a vital cog in the working of digital society for decades. Avast Blog identifies eight decades of progress within the field (2020):

1940s:

Cyberattacks were few and far between in the time between the creation of the first digital computer in 1943 and the following couple of decades. Only a limited number of people could access the giant electronic machines, and they weren't connected to networks.

1950s:

The term phreak refers to an individual interested in telecommunication systems. "Phreaks...used to hijack the protocols that allowed telecoms engineers to work on the network remotely to make free calls and avoid long-distance tolls", effectively engaging in one of the first forms of cybercrime. Although the practice has died out, the phreaks created a culture of interest in phone technology. Apple's cofounders Steve Wozniak and Steve Jobs were part of the phreaking community.

"Phreaks...used to hijack the protocols that allowed telecoms engineers to work on the network remotely to make free calls and avoid long-distance tolls"

1960s:

Hacking had become more prevalent as access to computers rose due to decreased cost and size, but "the attacks had no commercial or geopolitical benefits". Most hackers, often students, were doing it for entertainment or engaging in white-hat hacking, hacking attempting to improve upon security flaws in a system. Many companies had begun investing in data storage and management technologies due to the increased necessity of keeping information private.

1970s:

ARPANET (The Advanced Research Projects Agency Network), a prototype of the internet operated in the US during the early 1970s, gave birth to solid cybersecurity. It was financially supported by the United States Department of Defense, who understood how essential security for networks was.

Academic discussions about computer security took off in 1972-1974. The 1976 Operating System Structures to Support Security and Reliable Software report explained that "Security has become an important and challenging goal in the design of computer systems."

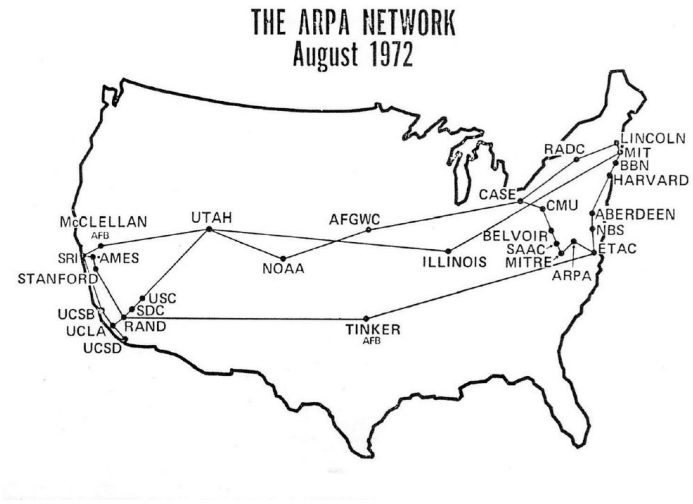


Figure 2: ARPA Network in 1972
(Computer Communications Review, 1990)

1980s:

An uptick in highly publicized cyber-attacks came in the 1980s, "including those at National CSS, AT&T, and Los Alamos National Laboratory". The terms Trojan Horse and Computer Virus were introduced in this era.

The US Department of Defence published the Trusted Computer System Evaluation Criteria in 1985, standardizing touchstones for trust in software and security in computer systems.

Security got a front seat in discussions of technology when, in 1986, German hacker Markus Hess hacked military and industrial computers connected to the ARPANET. Hess sold highly sensitive information to the Soviet KGB for US $54,000.

The first commercial antivirus was released in 1987, and in the following year a multitude of antivirus companies had been established worldwide. The early antivirus software often scanned code to find anomalies and deterred viruses by making it seem as though devices were already infected, although these "immunizers" quickly became unsuccessful as viruses developed.

1990s:

Early antivirus products were not always accurate and used lots of computing power, proving unpopular among users who valued productivity. Anti-antivirus programs and new virus techniques came about in the early 90s as a response by cyber criminals, rendering antivirus of the time ineffective.

New viruses and malware increased exponentially during the 1990s, “from tens of thousands early in the decade growing to 5 million every year by 2007”. The widespread requirement of security was apparent and firewalls, or networks that filtered traffic based on a system’s security rules, were beginning to be produced. Antivirus also evolved to evaluate all parts of code in which virus could be hiding.

2000s:

Cybercriminals had become more common with the spread of the internet and software vulnerabilities. Simply visiting a website infected with malware could put an entire system at risk. Instant messaging was also attacked.

Cloud computing was developed in this era, creating an on-demand solution to storage and centralizing server security. The Cloud continues to be used to this day.

Viruses that took up computing power were combated by new antivirus technologies. In 2008, the Anti-Malware Testing Standards Organization (AMTSO), an international non-profit, was created to test anti-malware technologies.

OS security, cybersecurity that is built into an operating system, was also introduced, creating a protected device to start. This introduced the practice of performing regular OS patch updates, installing updated antivirus software, firewalls, and securing “accounts with user management”.

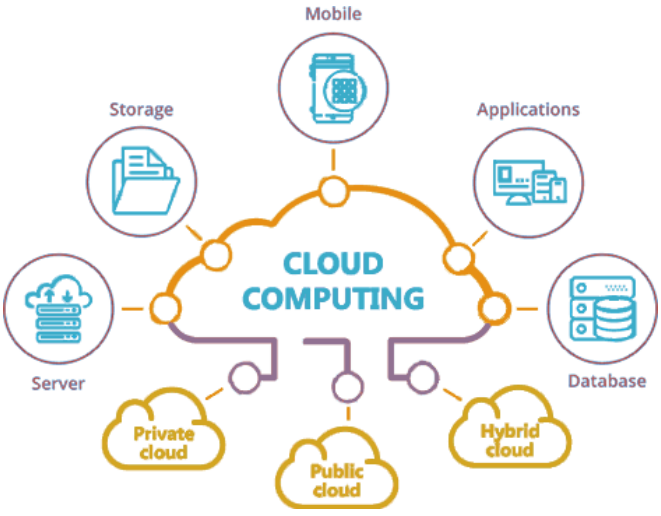


Figure 3: Cloud Computing
Network Encyclopedia [Online]

2010s:

Cybercrime in the 2010s severely impacted many countries' national security and "cost businesses millions."

Viruses have historically been extremely damaging and costly. The Melissa Virus of 1999 sent copies of itself through email, causing over US $80 million in damage according to the Federal Bureau of Investigation. The Saudi hacker 0XOMAR leaked the details of over 400,000 credit cards in 2012. 3 billion Yahoo user accounts were compromised after a 2013-2014 hack, costing the company an estimated US $85 million. The highly publicized WannaCry ransomware attack in May of 2017 infected hundreds of thousands of computers, costing approximately US $4 billion in damage.

In 2013, former CIA employee Edward Snowden leaked classified NSA information, ironically revealing global surveillance initiatives undertaken by the NSA for American interests, bringing into question privacy and security in the context of government scrutiny.

Figure 4: WannaCry Ransomware (Kan, 2017)

Why have Cybersecurity Companies Failed in the Past?

it is essential to pay attention to politics and hacking to avoid failure in the cybersecurity market.

The development of cybersecurity companies is dependent on the policies in place. In the mid-1990s, the company RSA Security held a public campaign against the Clipper Chip. The United States' government relaxed export restrictions on products that used it - which prevented RSA Security from selling its software abroad. It ended up being acquired, although the company is still running today.

Hacking is another problem can cause failure for cybersecurity businesses. The Dutch company DigiNotar admitted that their servers were hacked in June of 2011 in a collapse that changed the digital trust market forever.

The Market Landscape

Cybersecurity aims to completely secure the access experience for users, and as the time has gone on, identity has been used to ensure it. Modern hacking consists of the malicious usage of identity to compromise cybersecurity, bringing the need for digital trust.

A 2021 P&S report states that the Digital Signature Market is expected to generate over $25,211.3 million in revenue by 2030 (P&S Intelligence, 2021). The report argues that “[d]ue to the burgeoning requirement for smooth digital transaction management and user authentication, the demand for digital signatures is rising rapidly.” Additionally, “[d]ue to the growing requirement for online transactions and secure connectivity and rising popularity of the remote working culture, the market is exhibiting huge expansion.”

Defining Digital Trust

What Is Digital Trust? How Is It Different From Physical Trust?

Defining trust is difficult, and not just in the digital space. In the article “Trust and Accountability in a Digital Age”, philosopher Onora O’Neill states that trust is often considered a “generic attitude” that can be measured through reputational evidence. This is often measured through polling, and subjective measures based on public reputation can hardly work to place trust in a person, institution, or belief. Much of the reputation leading to trust may be ill earned or manipulated for the public eye. Thus, O’Neill argues, trustworthiness is more important than trust. Trustworthiness relies on evidence that is gathered through both a contextual lens which can consider “culture, gesture or tone”, as well as an empirical lens that “requires time, expertise or systemic investigation” (O’Neill, 2020).

The rapid increase of digitization in the past couple of decades brings forth the challenge of translating previously physical trust systems that dictated social interactions and economic transactions into the digital world. The article “On the Trust and Trust Modelling for the Future Fully-Connected Digital World: A Comprehensive Study”, conducted by a team of analysts at Huawei, defines digital trust as “a ‘measurable belief and/or confidence’ that is ‘accumulated from past experiences’ and is an ‘expecting value for the future’…” (Ting, et al., 2021). This definition implies that experience is vital evidence of trustworthiness. The ability to predict future action becomes more accurate with past behaviour in mind. Furthermore, reputation goes a long way in making its owner trustworthy. Finally, knowledge of the trustee and their environment is vital in trusting them during a specific situation.

Together, Experience, Reputation, and Knowledge work to provide trustworthiness. The clearest example of this is when a device attempting to authorize a user must be able to trust that individual based on their identity and behaviour to rule out the possibility of the user causing harm, a relationship that the study classifies as “Thing to People trust”. Experience factors in this situation can be evaluated through conflicting data on behaviour based on a user profile. Devices can detect uncharacteristic user behaviour based on their level of access. Reputation factors view a user as a part of an interconnected network, and anomalies in their role or connections can be an indicator of attempted misconduct. Finally, Knowledge factors consist of authenticating the user and assessing their features. Passing authentication is the primary way in which people can confirm that they are who they claim they are.

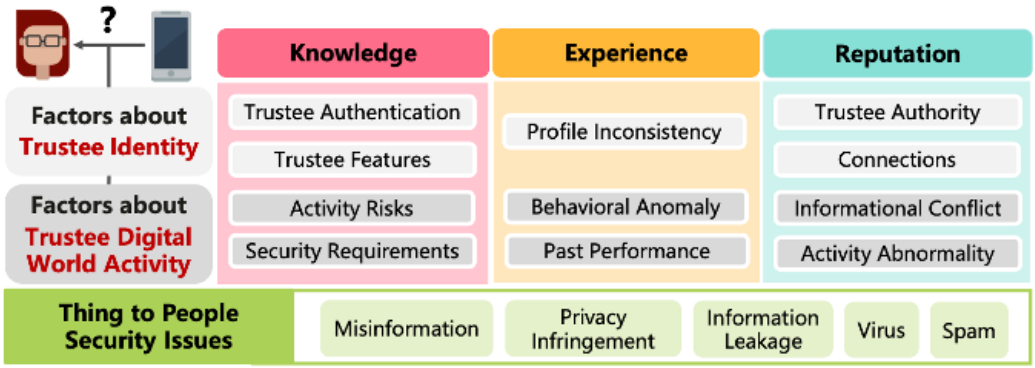


Figure 5: Thing to People Trust Factors
(Ting, et al., 2021)

Technology consulting analyst Sorell Slaymaker believes that digital trust is composed of two components: Mechanical and Relational Trust. Slaymaker defines mechanical trust as "the controls to deliver predefined outputs reliably and predictably and ensuring cybersecurity in the digital world." Mechanical trust can be delivered through advances in ensuring user identity and stricter security. Relational trust is "the unwritten promise to abide by the social norms in the evolving relationship between the customer and the digital enterprise." This trust can be forged with careful privacy policies that emphasize transparency and ethical applications of new technology (Slaymaker, 2020). Just as people use their knowledge of situations, experience with similar ones, and consider the reputation of involved parties on a day-to-day basis when making decisions about who to trust, devices are trained to use these factors to establish trust. However, we know that technology reflects the biases of those that create it. The individuals designing digital trust are just as vital as the technology itself.

In other words, mechanical trust depends on the deliverance of appropriate relational trust. If the creator of technology and the consumer cannot come to an agreement about how trust should be established, mechanical trust is the easy part. Relational trust depends on the market and the players in it.

What Current Technologies are Used for Ensuring Digital Trust?

PKI is a system that establishes and manages Public Key Encryption by using procedures, policies, and technologies to allow people and devices to encrypt and decrypt data. It can be used to issue digital certificates that authenticate the legitimate identity of users, devices, or services. The PKI system uses asymmetric cryptography to provide "identity and access management for a secure network" (Ludin, 2021). Asymmetric cryptography requires a private key and a public key. The public key is widely available for anyone to use in order to encrypt information. This data can only be accessed by the intended recipient, who owns the private key necessary to decrypt it.

Certificate Authorities, or CAs, issue certificates to validate the authorization of a public key owner. The public key owner will provide its public key and details, with which the CA can approve a certificate using their own private key. When the certificate is official, private key users can acknowledge the public key owner's reliability (Ludin, 2021). One of the most common uses of digital certificates is to validate websites and assure users that the public key encrypting their information is valid.

Modern cyber security attempts to think outside of the box when dealing with novel threats. Common technologies are:

- Multi-factor authentication (MFA), a widely known form of digital trust that verifies human identities through multiple things a user has or knows.
- Network Behavioural Analysis (NBA), which identifies dangerous files based on unusual behaviour.
- Threat intelligence identifying potential threats and the automation of software updates.
- "Real-time protection...on-access scanning, background guard, resident shield and auto-protect" are built-in security features in antivirus that scan for viruses in real-time.
- Sandboxing, in which a safe testing environment free from external factors can simulate running suspicious files or URLs.
- Forensics, during which security analysts can replay attacks to understand them and prevent future ones.
- Back-up and mirroring, in which files can be copied for safe keeping in the case of loss of information.
- Web application firewalls (WAF) that filter HTTP traffic as it flows in and out of web services. These protect "against cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection." (Avast Blog, 2020)

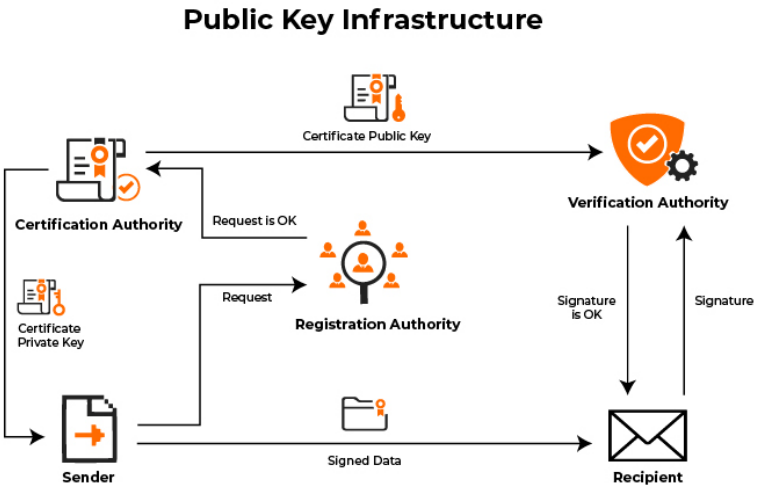


Figure 6: Public Key Infrastructure AppViewX [Online]

Why Is Digital Trust Becoming More Important Nowadays?

Digitization brings with it the inevitable rise of cybercrime. Wide-scale hacks and the loss of confidential sensitive information brings about the question of how to secure that information more meaningfully. In the United States in 2021 alone there were many devastating cyber-attacks at JBS, the Colonial Pipeline, Brenntag, Acer, Washington DC Metro Police Department, Steamship Authority of Massachusetts, and Quanta. According to European Commission, there are three parts of cybercrime: traditional crime (i.e., digital forgery/fraud), illicit content (i.e. incitement of bigoted violence, child sexual abuse material), and cyber-specific crime (i.e. DDoS, hacking) (Tsakanyan, 2017). The greatest growth in cybercrime comes from people-based attacks, which targets weaknesses in human security, including ransomware and malicious insider attacks, according to a 2019 study by Accenture. The research concluded that if nothing was done to prevent these attacks, the estimated cost of cybercrime would be $5.2 trillion by 2024 (Bissell et al., 2019).

In The Speed of Trust, author Stephen M.R. Covey proposes a way of looking at general trust that makes its effects tangible, through a formula in which Trust is correlated with the outcomes of Speed and Cost. Low Trust translates to low Speed and high Cost and high Trust translates to high Speed and low Cost (Covey, 2018). Thus, Trust and Speed have a positive correlation, while Trust and Cost have a negative correlation. One example of this relationship that Covey provides is the cause and effect of the Sarbanes-Oxley Act. This law, passed in 2002, intended to amend low trust in corporations because of their fraudulent financial reporting brought to light in a series of highly publicized corporate financial scandals in the early 2000s. To restore public trust in corporations, the law required intensive adherence to its regulations, many of which were time-consuming and cost high amounts to implement. If trust is low, repairing trust must be an arduous process. Covey also presents an instance of high trust saving money and time with the case of Berkshire Hathaway’s acquisition of Wal-Mart. The two parties were trustworthy and were able to take each other’s words to close the deal, saving months and millions (Covey, 2018).

Along with safety, trust undoubtedly provides the benefits of high speed and low cost. More users accessing the digital space for various reasons means more personal data stored. The longstanding controversy over technology companies' collection and distribution of personal data with little to no legal constraints is a primary example of trust being breached. Without safeguards in place to prevent both legal and illegal ways in which users are taken advantage of, the digital space will no longer harbour a safe space for people to conduct their affairs, whether personal, financial, or social.

"61% of Americans believe strong online security is the most important part of an app or website, while 52% say good privacy protections are the most critical."

Is There a Need for Digital Trust?

Digital trust is extremely important. In the growing market for online business services, customers expect the online security of apps and websites to be secure. According to a study by Okta, a company that has been successful in the world of digital authentication, "61% of Americans believe strong online security is the most important part of an app or website, while 52% say good privacy protections are the most critical." Additionally, "23% of Americans say good security (e.g., MFA offerings, secure log-in options) is critical to brand trust" (Okta, 2021).

If trust is severely violated, consumers are likely to look for alternatives (Slaymaker, 2020). Making systems more trustworthy will encourage consumers to use those systems in order to keep their information safe. In the digital world, trust between two parties is vital to key outcomes such as speed and cost, like Covey suggests. For example, if certain authentication actions or things inherent to one's identity were trustworthy, entering the digital space can become a faster and safer process that costs less for users to access.

Still, many confounding factors to establishing digital trust exist. Thanks to the ease of use of password-saving cookies, quick biometric scans such as face and fingerprint recognition, and one-click information access, consumer preferences have evolved to value convenience over zero-trust security. Okta (2021) found that “53% of 18–24-year-olds are unlikely to buy something from a brand they don’t trust, compared to 89% of 55+ year olds. Why? Millennials and Gen Z have grown up dependent on technology, and early exposure to handing over data means they may be more comfortable taking chances now.” Along with increased expectations of convenience, lack of accessibility to digital technology continues to be an issue that many people face. Bridging the digital divide across socio-economic classes should be a priority with establishing digital trust, meaning that costs need to stay low, and reach should be wide. Determining how digital trust should be provided and who provides it is a continuing debate with no clear answer. Still, the rise of crime and the necessity for awareness among consumers of digital technology remains, cementing a need for trust.

Consuming Digital Trust Technology

Are users aware of what data they are giving away? Do they/should they care about the potential risks of their data being collected?

When companies are not transparent on how a user’s data is going to be collected, used, and/or shared, users have no reason to trust companies with their personal data. Companies should take steps to ensure that users are aware of how companies use personal data, give users control over their personal data, and deliver value in return. These steps are crucial to building trust amongst users (Morey, et al., 2015). Value is a very open-ended concept and what it means in this context is a more convenient and personalized service facilitated by a user’s personal data (Morey, et al., 2015).

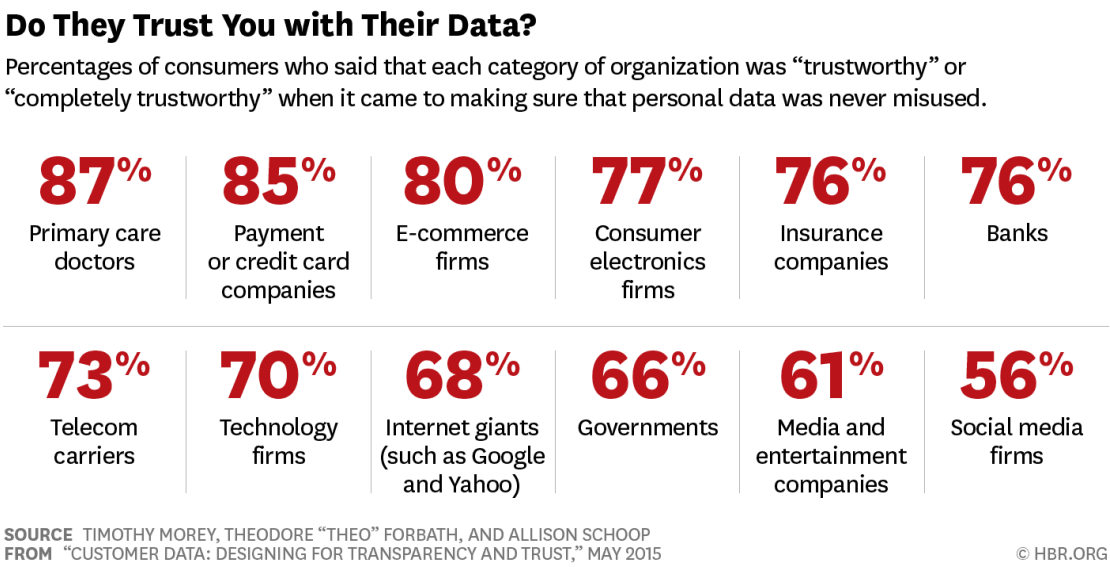


Figure 7: Users' trust in organizations
(Morey, et al., 2015)

For instance, the music service Pandora gathers a few details about the user including their gender, age, and location. Pandora also keeps track of a user's listening activity, community posts, device information, etc. which it uses to better personalize the music to the user and to serve targeted ads (Pandora, 2021).

The value of personal data is a topic that has been hotly debated since the birth of the digital age, and understandably so. Businesses trying their best to determine what will sell the best, what people are looking for, and what they are interested in buying. The best way to collect these details would be to examine a user's browsing patterns, interests and other information they may be knowingly, or in most cases, unknowingly giving away. But to what extent are users giving away their information, and should they be worried about it?

According to a study conducted by Pew Research Center, it was found that most adults are not aware of many aspects of data collection and the study had quite a few findings which will be discussed throughout this paper. While this study was conducted in the United States of America, it is not unreasonable to assume that this study will depict a realistic portrayal of privacy and security all around the world.

The study found that the majority of Americans (over 60%) do not think they are in control of their data and that they cannot go about their lives without their usage being tracked and their data being collected due to how prevalent data collection is in online services nowadays (Pew Research Center, 2019). Most users, however, do not realize that data collection is vital for the operation of many services we need on a day-to-day basis.

From data collected to improve user experiences for many software and services, to medical research using patients and caregivers' data, it is evident that there are benefits of data collection in many sectors (ENISA, 2018).

It is easy to be worried about data collection as it is very commonly associated with ad revenue or businesses, and with the rising number of data breaches and exposed records (Statista, 2021), users do not have much reason to believe that their personal data is collected, used, and handled safely or whether this data collection is even necessary. According to the study conducted by the Pew Research Center, this is a cause for concern for many users as they worry that the risks of data collection and data usage outweigh the benefits. The users also say that they gain little to no benefits from this data collection by companies and the government (Pew Research Center, 2019).

Many users do not understand the frameworks in place concerning privacy. The study conducted by the Pew Research Center found that over 60% of adults have little to no understanding of the laws and regulations in place concerning their privacy and their rights.

Part of the reason for this statistic is that many users do not read privacy policies before agreeing to services. Further contributing to this statistic is the nature of most privacy policies, resulting in most users not understanding its contents. Only about 20% of adults admitted to reading privacy policies to completion (Pew Research Center, 2019).

The study also found that their willingness to contribute data greatly depended on the context and reasoning provided. For instance, users were far more willing to share their data with the government to assess potential terrorist threats, but not as much when they were asked if they would share their data with social media companies to detect signs of depression. (Pew Research Center, 2019)

In a similar study conducted by Malwarebytes, it was found that only about 30% of users read through End User License Agreements for a software or service before agreeing to its terms (Malwarebytes, 2019). This is not a promising statistic as these policies often contain details about how data will be collected and used and may include agreements on what other applications or services have access to your data.

Britain's Channel 4 has found a good balance between making users understand their data collection and privacy policy whilst not overwhelming them with details. The TV station has a dedicated website to inform the user about the data they collect, why they collect it, and who they share it with. They go on to reassure the user about their rights to their data stored and explains that it can be deleted from their system upon request (Channel 4, 2021). These approaches can go a long way in increasing a user's trust in a company, with Channel 4's director of viewer relationship management stating that 11 million viewers have registered on the site. 80% of users have also chosen to volunteer their address details despite not being mandatory and fewer than 0.01% opt-out of targeted advertising (Morey, et al., 2015). According to the Malwarebytes study, a significant number of users (nearly 30%) were not aware of the permissions they had granted to apps on their mobile phones (Malwarebytes, 2019). This is a major problem as there have been applications requesting and being granted unnecessary permissions in the past, the most notable example being flashlight apps needing access to substantially more permissions than they would need (Miliefsky, 2014).

Many users are not aware of quite how much data they give away when they do simple actions from merely browsing the internet to searching for a new pair of shoes (Morey, et al., 2015). Most browsers and apps often give away details including your location, the browser you use (if applicable), your device's battery level (if applicable) and other device hardware information, your clicks/taps, your browser/app movements, etc. (Linus, n.d.).

To start with, browsers and apps collect a bunch of details about your device, including the aforementioned location, browser/app information, other hardware information, etc., to create a "digital fingerprint" of the user. This can be used to uniquely identify a device, and indirectly a user as their usage patterns will be reported by the device. This digital fingerprint can be used to serve the user more personalized ads, personalisation, and recommendations which in turn can be used by companies and data brokers to make money off your data (Briz, 2018). In 2017, it was estimated that the average revenue generated per user in the digital advertisement space was $59 per person. It is then easy to why there is an entire business model based on user data. (ENISA, 2018)

How can a company enhance their security systems whilst providing a positive user experience?

A clear indicator of digital trust is user action (Bhalla et al, 2021). If a user judges their online interaction with a company to be insecure or overly complicated, they are not likely to continue their interaction with this company. Due to this reason, all cyber security businesses that aim to promote digital trust must strive for a dual goal: they must maximise security, whilst ensuring a positive user experience. The difficulty of achieving these goals simultaneously should not be underestimated.

It is generally agreed that in order to establish digital trust, a company has to demonstrate a commitment to installing sufficient security measures (Bhalla et al, 2021). As mentioned previously, security measures, such as a high level of authentication, are put in place to protect company and client data, and have previously been achieved by Customer Identity and Access Management (CIAM) solutions. Often delivered as cloud-based services, CIAM solutions aim to provide high levels of security using features such as Multi-Factor Authentication (MFA).

With MFA, a customer is required to provide additional information, such as a security answer or a one-time code sent to their mobile device, to access their data. Whilst CIAM solutions promote the enhancement of security systems, the additional security measures infringe on the user's experience. This is because Knowledge-based authentication, such as security questions, may be difficult to remember, whilst SMS Two-Step Authentication can be inconvenient if the user cannot access their mobile device. Whilst security may be a priority for companies and some clients, user experience should not be overlooked (Pinkham, 2019). We can return to our previous statement that "a clear indicator of digital trust is user action" to suggest that companies should provide a flawless customer experience in order to establish digital trust and to generate revenue (Bondar et al., 2021).

"[A] clear indicator of digital trust is user action"

Additional inconveniences (a loss of time) that arise from increased security measures such as CIAM solutions may lead to a negative user experience, to the extent that enhanced security would no longer be necessary, as clients would stop using the company's platform due to frictions.

The importance of convenience for a digital user has been highlighted by a study looking into satisfaction rates during mobile banking in Pakistan (Fiaz et al., 2014). The results of this study concluded that user satisfaction was primarily determined by the ease of use of e-banking platforms. The importance of simplicity and convenience has been further supported by British surveys looking into the impact of two-factor authentication on user experience: the respondents of these surveys expressed their frustration about providing additional information whilst online banking (Svilar and Zupančič, 2016). Such results may suggest that for some individuals, practicality overrides higher levels of security. Consequently, it can be argued that providing a flawless customer experience, whilst maintaining high levels of security, should be the real priority for digital trust companies, as it will encourage customer loyalty and therefore generate higher revenue for the company.

This may initially appear to be an achievable agenda, but as we have highlighted, the trade-off relationship between high levels of security and a positive user experience complicates the establishment of digital trust. How can a company provide a secure online system without discouraging user engagement? One solution may a wide-scale implementation of biometrics, which would streamline the authentication process by reducing the amount of time and effort required to authenticate the user, whilst maintaining a high level of security. Passwords and security answers can be easily interpreted by sophisticated hackers, and therefore their vulnerability increase the risk of unauthorised access to data. On the other hand, the use of biometrics for authentication provides an additional level of security, as they are extremely difficult to hack, especially without physical interaction. This authentication process ultimately reduces friction for the user by establishing a streamline login experience and by providing security with simplicity (Zhao et al., 2019).

Risks

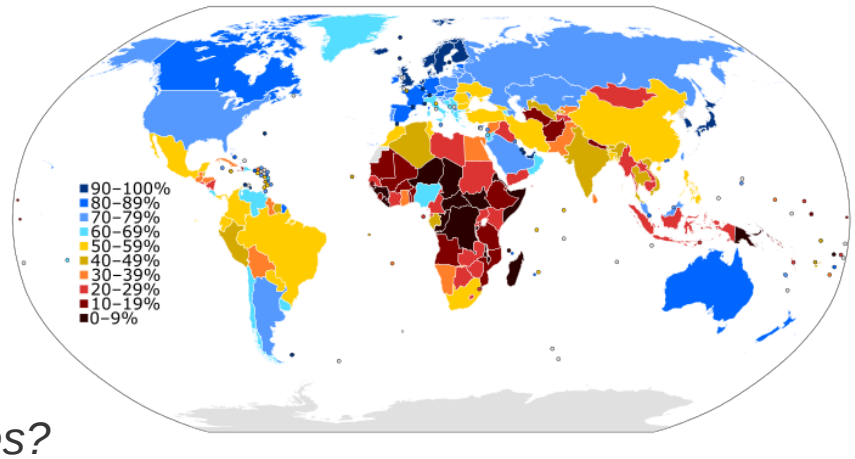


Figure 8: "Internet users in 2015 as a percentage of a country's population"
(International Telecommunications Union; Retrieved from: Wikipedia)

How does lack of access to digital trust versus access to digital trust result in inequities? How will these inequities be exacerbated or mitigated as the world becomes increasingly digitized?

Digital trust can already be difficult for many individuals to gain access to because of the *digital divide*: access to technology being affected by economic or geographic situations.

People without the ability to purchase personal devices or security services such as high-level encryption are more at risk to compromise their information and are also put at a disadvantage compared to those who can in terms of work or communication possibilities. In his book Enhancing Digital Equity: Connecting the Digital Underclass, Massimo Ragnedda introduces the idea of a Digital Oligarchy, in which cutting-edge technologies are primarily developed and controlled by wealthy and powerful organizations.

Few hi-tech companies, known as FAMGA (Facebook, Apple, Microsoft, Google and Amazon), are leading investments in AI and other technologies, consolidating their dominant position in the market and the whole of society" (Ragnedda, 2020). Ragnedda explains that this contributes to the failure of small innovative businesses that do not have the financial capital to survive bumps such as the COVID-19 pandemic, leading to acquisitions by the dominant companies. A pervasive industry such as digital trust would be even more difficult to revolutionize without the support of one of these companies, making quality trust even less accessible to the public, especially those without financial access to stronger security.

"90% of growth in the US tech sector between 2005 and 2017 occurred in five cities…making the city high-priced and unaffordable for more people."

Geographic location is also important to consider in terms of accessibility to technology. Technological hubs differ across nations and regions. Availability of networks and devices also differ based on one's location. Certain areas that are very well endowed historically tend to attract highly skilled workers and appropriate resources to determine world-changing technologies. (Ragnedda, 2020) argues that "90% of growth in the US tech sector between 2005 and 2017 occurred in five cities (Boston, San Francisco, Seattle, San Diego and San Jose) … this may intensify income inequality, making the city high-priced and unaffordable for more people." Thus, geographic inequality contributes to economic inequality and further to the digital divide.

Even without the inequalities in access to technology, access to digital trust can prove to be just as difficult in the same areas. A commonly used means of determining one's identity is legal certification of some kind. Government IDs or birth certificates are often suggested to take the role of authenticating someone, but issues exist. There may be individuals without issued or valid IDs and proof of birth that should still be protected in the digital sphere. Concerns about central authority's abuse of private information and tracking data also exist. Many individuals do not trust the government to assign and track identity efficiently or honestly. These proposed forms of identification also bring into question the socio-economic risks and benefits to users of such a system and how it should be enforced.

What are the socio-economic risks & benefits of a digital identity system?

In 2006, Clive Humby famously referred to data as being "the new oil" (Humby, 2006). This concept is still referenced fifteen years later, and it has highlighted the complexity of achieving digital trust and the value of data possession within the 21st Century.

The wide-spread implementation of digital identities has been pursued by a variety of actors, from governments to private corporations, as we currently live in a data-driven world, in which the supervision of data can not only ensure a company's long-term survival, but it can also provide substantial socio-economic benefits for communities. To assess the future of the digital landscape, it is necessary to consider the opportunities and implications that may arise from a global implementation of digital identities.

A digital ID in this context refers to a universal document that can be used to verify an identity on a digital channel (White et al., 2019). By digitalising identity systems, governments aim to promote efficient operations by removing the complexity of providing different physical identification documents for every new online service (White et al., 2019). Similarly, businesses want to establish a seamless customer identification process through the development of digital identities and digital verification services to enhance user experience and to promote digital trust, as users are given greater levels of control to manage their own data (Pinkham, 2019).

The economic decline following the COVID-19 outbreak has accelerated the shift towards digital identities in the UK, as digital ID schemes are considered to drive innovation and business growth, therefore playing an instrumental part in the country's economic recovery process (Bar Am et al., 2020). This theory can be supported by a recent McKinsey Global Institute report, which stated that the adoption of a digital ID scheme can boost a country's GDP by 3 to 13 percent by 2030 (White et al., 2019).

This would be a result of reduced levels of fraud, an increased use of financial services and a general improved efficiency: it is estimated that digital IDs would lead to a 90% reduction in the cost of online consumer registration and verification (White et al., 2019). The socio-economic benefits of state-level digital ID schemes have been demonstrated by Estonia, the world's most advanced digital society. With around 99% of the country's public services being accessible online, Estonia has promoted social and economic inclusion by connecting individuals to governments and businesses to consumers (Anon, 2019).

However, in order to reap the socio-economic benefits of digital ID systems, a digital trust framework would need to be established, which is a complex task due to the privacy concerns surrounding digital ID schemes. For example, India's digital ID scheme, Aadhaar, has been widely criticised for being vulnerable to unethical commercialisation of biometric data and for enabling unauthorised use of biometrics, leading to identification without consent (Satpathy, 2017). This ultimately highlights the potential for digital identification systems to violate individuals' fundamental right to privacy, as they do not have control over how their personal data is handled.

Based on these implications, it appears reasonable to suggest that in order to establish digital trust, digital identity schemes must be based on data sovereignty. For example, consumers must not only have control over who can access their data but should also be allowed to revoke this access and demand the deletion of their data (Huang and Yuan, 2020). Promoting transparency and data sovereignty in the design of digital identity programs will establish trust. Without digital trust and confidence of data privacy, the public will not engage with a digital identification system, no matter how "seamless or frictionless" it may be (Anon, 2020).

Regulation

How do we work to provide regulatory access to encrypted information to governments or investigations?

The debate of whether to provide regulatory access to encrypted information and data to governments and law enforcement is long-standing. Governments and law enforcement have fervently demanded access – claiming that it is necessary to prevent crimes, including drug and human trafficking and terrorism. On the contrary, private cybersecurity companies and multitudinous independent human rights organizations and research institutes have argued that allowing unabridged access, whether through encryption backdoors or key escrows, would infringe upon individuals' right to freedom of expression and privacy, while also creating increased opportunities for hackers to access and publish confidential material.

Recent occurrences within the cybersecurity realm, specifically in the mid-2010s, have reignited the fire fuelling this debate. After whistle-blower Edward Snowden produced evidence of various governmental operations that infringed on the privacy and security of individuals across the globe – including the 2013 Guardian report wherein documents were leaked showing National Security Agency (NSA) collection of telephone records from millions of Verizon customers, as well as the revealing of Britain's Government Communications Headquarters (GCHQ) tapping fibre-optic cables to collect and store global data, then sharing it with the NSA – many were outraged and were highly in favour of maintaining end-to-end (also known as "warrant-proof") encryption to protect their personal and professional communications (Szoldra, 2016).

However, prevailing opinions were challenged following the 2015 attack in San Bernardino, California, wherein 14 people were killed and 22 seriously injured. Following the attack, the Federal Bureau of Investigation (FBI) had found the iPhone of one of the attackers and sought to decrypt the information; however, Apple refused to aid the FBI in breaking into the phone, claiming it would set a “dangerous precedent, making all iPhone users vulnerable,” (The Associated Press 2016). Many, especially those in government and law enforcement, were outraged by Apple’s refusal to break into the phone, especially since the attack had been linked to terrorism. Throughout this section, the arguments of both sides will be analysed and the potentiality of a solution that serves the interests of both sides will be explored.

Relevant Terminology

Encryption: According to the SANS Institute, encryption is defined as “a mathematical process of converting message, information or data into a form unreadable by anyone except the intended recipient” (2001). Moreover, as iterated within the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, published by the United Nations Human Rights Council, encryption works to “protect the confidentiality and integrity of content against third-party access or manipulation [in transit and at endpoints],” (Kaye, 2015). Examples of end-to-end encryption platforms include WhatsApp, Facebook Messenger, Viber, and Kakaotalk (Espinosa et al. 2017). Furthermore, it is important to note that encryption does not protect “identifying factors such as the Internet Protocol (IP) address, known as metadata,” (Kaye, 2015).

Key Escrow: A key escrow is a third-party database wherein the encryption key for a particular set of data is stored. If a court were to subpoena information from this database, the key in escrow would be duplicated and the court would have access to the encrypted data (Nohe, 2020).

Case 1: Those in Favour of Allowing Governmental/Law Enforcement Regulatory Access to Encrypted Data & Reactions – in the Context of the "Five Eyes" Group

Prior to 2019, Canada remained steadfast in their commitment to end-to-end encryption, as expressed by Minister of Public Safety Ralph Goodale in his briefing notes at the Five Country Ministerial (a meeting of the "Five Eyes" Group) in 2017. In these notes, Goodale explains that though "encryption poses challenges for Canadian law enforcement investigators, it also safeguards our cybersecurity and our fundamental rights and freedoms," (Parsons 2019). These notes reaffirmed Canada's cybersecurity standpoint, which ran counter to that of the other countries (Australia, United States of America, New Zealand, and the United Kingdom) that make up the "Five Eyes" Group.

However, in 2019, the tides changed, with Canada now holding a stance contradictory to what they had in the past.

In the 2019 Five Eyes Meeting Communique, all the national ministers asserted that cybersecurity and technology companies should be including backdoors/key escrows into their security systems so that governments "with appropriate legal authority, can obtain access to data in a readable and usable format," (United Kingdom's Attorney General's Office and Home Affairs, 2019). After the release of the communique, Goodale even went on to paint end-to-end/ "warrant-proof" encryption systems "as the preserve of those who would exploit children, for example," despite having openly spoken about the necessity of "strong encryption" to the same group only two years prior (Thomson, 2019). Goodale's (and de facto the Canadian government's) acquiescence to support access to encrypted data was met with much discontent. The Citizen Lab, a research laboratory located at the University of Toronto, called out Minister Goodale in a 2019 article for using lack of access to encrypted data as a scapegoat for crimes such as child abuse/exploitation.

They noted that Goodale's comments following the release of the communique "insufficiently communicate the baselines failures within the Government of Canada", highlighting their failed utilization of available data and resources to conduct investigations into such crimes (Parsons, 2019). Moreover, in the same article, Citizen Lab cites a meta-analysis of Attorney General and provincial annual reports on electronic interception reports. This analysis presents that from 2005-2014/16, none of the reports indicated that encryption prevented interceptions from taking place (Parson, 2019) – weakening Goodale's claim that lack of access was detrimental to conducting investigations and/or intercepting information for the purpose of law enforcement.

Another nation within the "Five Eyes" Group, the United States, recently tabled legislation that demands regulatory access to encrypted data by central authorities. The Lawful Access to Encrypted Data Act, introduced on June 23, 2020, is described as "a bill to bolster national security… by ending the use of 'warrant-proof' encrypted technology by terrorists and other bad actors to conceal illicit behaviour," (Committee of the Judiciary, 2020).

Many individuals are not in support of this bill, as they claim it infringes on their rights to freedom of expression and right to privacy; however, the tabling committee has rebutted these claims, responding with a gleaming list of benefits that the Act would introduce. Such benefits include an increase in technological innovation (via a direction to the Attorney General "to create a prize competition to award participants who create a lawful access solution in an encrypted environment") as well as the promotion of "technical and lawful access training and the provision of real-time assistance" (Committee of the Judiciary, 2020).

Though many articles have been released following the tabling of this legislation, it is a 2016 report by the Berkman Institute for Internet and Society at Harvard University that, ironically, best responds to the drafters' concerns whilst promoting end-to-end encryption to protect individual and private entities. The report, entitled "Don't Panic: Making Progress on the 'Going Dark' Debate", explains through various articles that though encryption does prevent governments and law enforcement from intercepting private messages, they are not at a loss for data collection and crime-stopping.

Metadata (e.g., location data from cell phones, telephone calling records, header information in an email) is not encrypted; thus, it can be utilized by governments and law enforcement. Moreover, as networked sensors, video/sound technology, and the Internet of Things expand, there will be further opportunities for surveillance; hence, governments should lessen their fears of a world "going dark," (Olsen, Schneier & Zittrain, 2016). In closing, the report iterates the focal issue of regulatory access for governments and law enforcement: "backdoor accesses built for one purpose have been surreptitiously used for another," (Schneier, 2016).

Case 2: Human Rights Organizations and Legislative Bodies Not in Favour Allowing Governmental/Law Enforcement Regulatory Access to Encrypted Data

Many human rights organizations and legislative bodies have spoken out against allowing government/law enforcement regulatory access to encrypted data, including the Electronic Frontier Foundation and the American Civil Liberties Union. However, for brevity's sake, this section will focus predominantly on the Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (herein referred to as "the Report"; 2015), published through the United Nations Human Rights Council (UNHRC), as well as opinions from the European Union (EU) Working Party 29. According to the Report, encryption and anonymity "provide individuals with a means to protect their privacy [whilst] empowering… and enabling journalists … [and] those persecuted because of their sexual orientation or gender identity, activists … to exercise the rights to freedom of opinion and expression," (Kaye, 2015). Moreover, it rejects unabridged and continual access to encrypted data, even for "lawful" or governmental purposes, citing Article 17(2) of the International Covenant on Civil and Political Rights – a United Nations treaty which all of the countries party to Five Eyes group have ratified (Kaye, 2015). Article 17(2) states that member states should "ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy" and that "individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption …" (Kaye, 2015).

Similar to the Covenant, the Report does not outrightly reject the decryption of data, suggesting it only be “permissible when it results from transparent and publicly accessible laws applied solely on a … case-by-case basis to individuals … and the protection of due process rights of individuals;” however, it places greater emphasis on the encryption of data for the purpose of individual safety and security whilst encouraging “better digital literacy” and the provision of encryption and anonymity tools to internet users (Kaye, 2015). A legislative body that holds similar sentiments to the UNHRC Report is that of the EU Working Party 29 (now replaced by the European Data Protection Board). When faced with the question of whether governments and law enforcement should have regulatory access to encrypted data, their reply was cogent and concise. The Working Party opined that the imposition of backdoors or key escrows for regulatory access would only endanger the “honest citizen,” causing them and their data to become increasingly vulnerable to online criminal interference (EU Working Party, 2018).

Business Considerations

Can money be made from digital trust?

The success of a business is influenced by many internal and external factors that cannot always be controlled by the employees of the company itself. For example, Baltimore Technologies was an Irish firm leading internet security just before the 2000s, focusing on PKI software implementation (Baltimore Technologies plc, 2002). Their timing entering the cybersecurity market was advantageous because there was a need for digital trust especially during the internet boom (Reference for Business, 2002). Furthermore, the company also managed to secure high profile contracts with Governments and large companies such as the Bank of America, which established Baltimore Technologies' brand name worldwide (Reference for Business, 2002).

However, external factors can also be detrimental to the profitability of a business. In March of 2000, Baltimore Technologies succumbed to the collapse of high-tech stock prices, leading to a 900% increase in losses the following year, along with a slump in internet-based economy (Reference for Business, 2002). Larger companies took advantage of the opportunity to acquire Baltimore Technologies, taking over their innovative technology and ceasing the existence of their trademark. Digital trust and cybersecurity is, unsurprisingly, a very large field that encompasses a variety of different business sectors including banking, manufacturing, retail, telecommunications, transportation (Grand View Research, 2021).

The area of digital security also includes different use-cases, as illustrated in Figure 9, created by the cybersecurity software company Aretiico.

Different use-cases require different solutions as well as business models. For example, hospitals are considered as critical infrastructure in many countries, which is why data access relating to healthcare must be very secure (Gomes et al., 2017). An incident regarding an important use-case occurred in 2016 when the electrical power control system in parts of Eastern Europe was compromised by attackers, cutting electricity to 230,000 people (Booth et al., 2020). Any breach in security with these critical infrastructures can lead to disruptions in essential services and severe effects in the community, which is why cybersecurity solutions for these use-cases must be detailed and robust (Gomes et al., 2017).

On the other hand, use-cases such as secure browsing and ordinary app data storage still require digital security to a certain extent, but clearly do not have as severe consequences as those relating to critical infrastructure or financial transactions.

Cybersecurity companies can make money through a variety of ways, depending on their values, mission statement, core competencies and how they operate as a business. Large companies are more likely than smaller companies to provide a wide range of services since they have enough resources to do so. All of these services include having clients, who can be Governments, companies, or lone consumers.

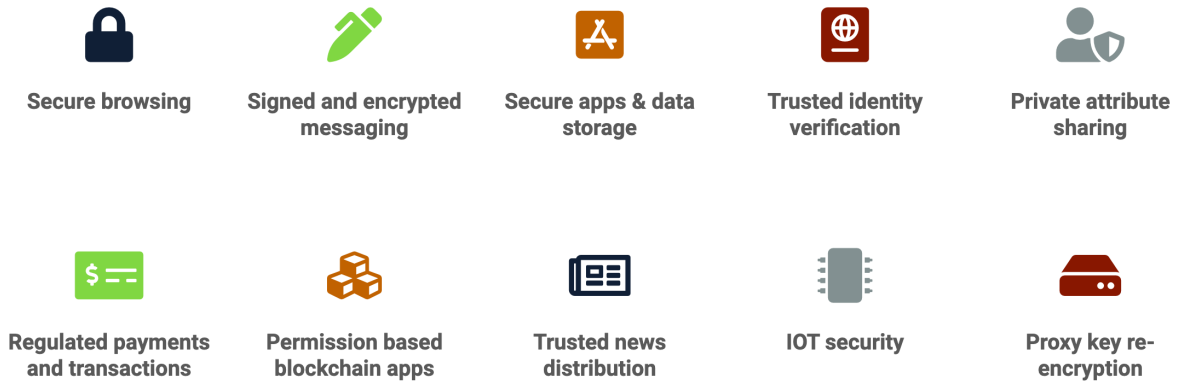


Figure 9: A few use-cases of digital security
(Aretiico Ltd., 2021)

Some examples of services include IT consulting, penetration testing (seeing whether a client's security system is vulnerable or not), systems auditing (checking whether a client's security system is complying with legal standards), and developing an innovative security system (Day, 2021). Companies can also make money directly from newly developed digital trust systems, such as charging money for each digital trust certificate that is issued by a Certificate Authority (Day, 2021). According to Booth et al. (2020), the difference between cybersecurity professionals and unfilled job positions will be around 1.8 million in 2022. A variety of cybersecurity breaches, including cyber-attacks as well as unauthorized access to confidential information, can cost the global economy as much as one trillion US dollars a year (Etzioni, 2014). A report by Sid Kircheimer (2013) also estimates that around 508,000 people have lost their jobs in America due to the effects of cybercrime (Etzioni, 2014). Companies are keen to reduce the potential of such losses in order to maximize their profitability and general reputation.

In addition, government regulations such as those derived from General Data Protection Regulation (GDPR) as well as The Communications Act require businesses to adopt security practices that protect company data and confidential information (McNicholas and Angle, 2020). A combination of needs and shortages indicate the demand for companies to outsource cybersecurity professionals, demonstrating why it is possible for cybersecurity companies to make money from digital security services.

What is there to consider when starting a cybersecurity business?

Digital trust is becoming more prominent nowadays, with a large enough market for customers. According to Grand View Research (2021), the global cybersecurity market is expected to have a compound annual growth rate of 10.9% from 2021 up to 2028, due to incidents relating to security infrastructure. The increasing prominence of data in the Internet of Things (IoT), especially boosted by the COVID-19 pandemic, has provided more opportunities for hackers to take advantage of technological vulnerabilities within companies (Grand View Research, 2021).

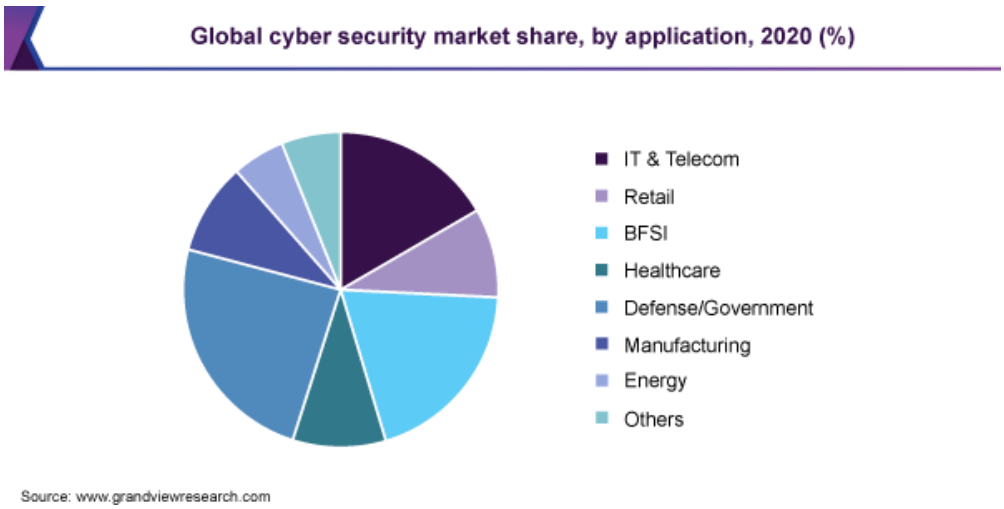


Figure 10: Global applications of cybersecurity and their market share (Grand View Research, 2021)

In China alone, the demand for cybersecurity services are around 700% greater than the number of trained security professionals (Shanghai Laoqin Information Technology Co., Ltd., 2019). There are also significant clients that cybersecurity businesses can target in this market. The pie chart in Figure 10 depicts the global market share for different applications of cybersecurity in 2020, where Government and Defence applications dominated the market with around 24% overall (Grand View Research, 2021). According to Gomes et al. (2018), Business to Business (B2B) and Business to Government (B2G) customers are growing, whilst attracting Business to Customer (B2C) has been quite difficult. This may change in the future as homes become filled up with IoT devices (Gomes et al., 2018). Digital security in healthcare is also expected to increase rapidly.

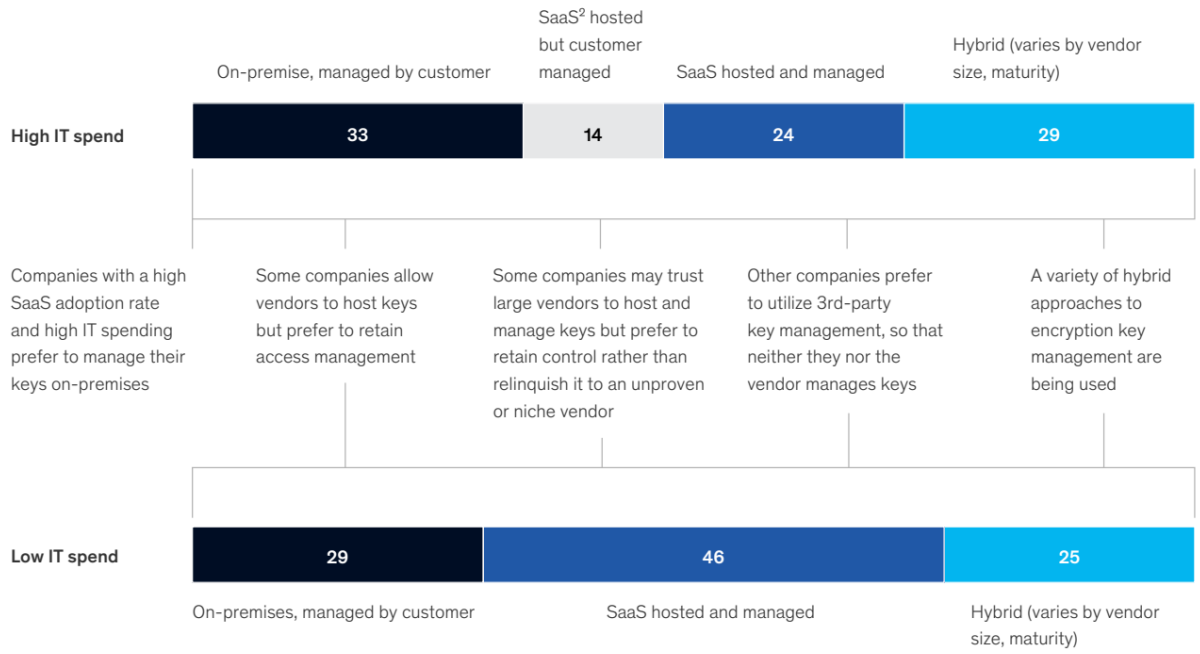
In places such as China, information security products are essential in applications relating to telecommunications and finance, which are the core of the country's existence (Forward Business and Intelligence Co., Ltd., 2014). The cybersecurity market is quite stable and will keep growing in the future.

In the cybersecurity field, companies should pay close attention to changing industry regulations, as they can severely affect the legality and profitability of digital trust businesses. It costs money to invest in technology to comply with regulations as well as perform audits (Booth et al., 2020). A digital solution for one client in the healthcare sector will not necessarily comply with laws in the financial sector, so cybersecurity businesses should fully examine the different fields that they target (McNicholas & Angle, 2020).

Nonetheless, in the USA and many parts of the world, there is no single Governmental law stating the specific cybersecurity practices that must be implemented by companies; the practices usually just need to be ‘appropriate’ enough to prevent cyber losses (McNicholas & Angle, 2020). Legislations can take months and years to develop through gaining approval from different political groups, and a grace period is also needed to allow businesses to adapt and adjust to changes (Prinsley et al., 2021). Varying requirements in different industries, as well as differing opinions, make it difficult for Governments to pinpoint a single, universal law for cybersecurity (McNicholas & Angle, 2020). One cybersecurity law that the UK Government is currently drafting involves banning universal default passwords (Prinsely et al., 2021). These laws are not necessarily up-to-date and are already implemented by the highly secure companies, not posing any threat to their operations.

However, cybersecurity practices are becoming more similar to each other as the result of tightened security and globalization. It is possible that a global agreement on some general practice regulation could become the norm.

For instance, the PKI Consortium consists of a group of leading Certificate Authorities (CA) and software suppliers that focus on creating best practice procedures for trust in the digital world (PKI Consortium, 2021). In 2016, this group implemented guidelines for companies to enhance digital security, including requirements like having a Time-Stamping Authority (TSA) (CA Security Council, 2016). Although these guidelines are not legal regulations for cybersecurity businesses, joining consortiums as members can help companies become more trustworthy to the public, increasing their sales and profitability in the long run. Since there are no highly demanding regulations that need to be followed, each individual client will desire to have a tailored digital security system that fits their needs, even if it is only slightly modified from the base digital solution. Some companies prefer to have their own in-house security system, as this allows for more flexibility and less dependence on third-party organizations (Grand View Research, 2021). As depicted below in the diagram, some clients also prefer having authoritative access over encryption keys, whilst others prefer for the cybersecurity or Software as a Service (SaaS) companies to be in control of them (Cracknell et al., 2020).



[1] All IT-spending estimates rely on information from "IT key metrics data 2019: Executive summary," Gartner, December 17, 2018, gartner.com.
[2] Software as a service.
Source: McKinsey Customer Perspectives on SaaS survey and interviews with more than 60 industry leaders

Figure X: Percentage of companies that want to manage encryption keys (Cracknell et al., 2020)

Therefore, clients have a lot of power to decide the cybersecurity features that they wish to have as a customer. It is also up to the company itself to decide whether they want to hire specialist cybersecurity firms to develop a secure system for them, rather than having their own technological division or Chief Information Security Officer (CISO). According to Etzioni (2014), some reasons for companies not adopting well-developed cybersecurity measures are because CEOs tend to underestimate the long-term negative externalities, and investing in security costs a lot of money.

As discussed previously, security solutions can be monetized and a market for digital trust definitely exists, but cybersecurity companies should be strategic by evaluating different needs from different customers, in order to tailor services to certain audiences and maintain high satisfaction in such a competitive market. Examining large global competitors in the cybersecurity market like Cisco Systems Inc., IBM and McAfee, may help cybersecurity start-up companies develop a business model that can penetrate the current market (Grand View Research, 2021).

What are the technical difficulties in creating a digital trust solution?

A lot of current cybersecurity solutions protect technology by disallowing outside data to enter the system i.e., by creating a firewall (Booth et al., 2020). However, firewalls are only preventative and can be ineffective against attacks that originate inside the system itself, such as viruses in a USB (Booth et al., 2020). Updating the digital security system will also require the technology to shut down temporarily, and many clients do not have sufficient backup systems to adapt to this change of situation (Booth et al., 2020). Many companies allow their staff to bring their own devices and use the company's network without having to carry out any cybersecurity checks, posing a clear threat to security (Booth et al., 2020). These are just a few technical difficulties that new cybersecurity companies may want to find a solution for.

Conclusion

Who should provide digital trust? A community? A government? Big tech?

There is debate regarding who should ensure trust in the digital field. Whilst trust may vary significantly on an individual's perspective and priorities, broadly speaking, a digital trust provider must promote transparency, they must reinforce ethical practises, and they must uphold high levels of security to achieve digital trust (Albinson et al.).

Estonia's successful implementation of digital identities could be largely attributed to the nation's high levels of governmental trust (Cater, 2021). However, it should be noted that there is "less emphasis on privacy [and] less emphasis on fighting against the government" in Estonia compared to the United Kingdom (Cater, 2021).

This suggests that digital trust systems that have proven to be successful in other nations may not have the same effect in the United Kingdom, as data protection regulations often reflect a country's own socio-cultural state of affairs. Furthermore, Estonia's digital ID scheme is characterised by centralised control points, and therefore comes with the risk of unauthorised surveillance (Goodell and Aste, 2019). This vulnerability suggests that complete governmental authority over data may undermine digital trust. This argument is supported by demands for governmental deregulation in data protection following the mediatisation of security breaches, such as the Snowden breach mentioned previously (Abraham et al., 2019). Due to these implications, it could be argued that digital trust should be ensured by corporations which acknowledge the significance of transparency. A recent report by the International Digital Corporation has highlighted the business ecosystem would benefit significantly from the establishment of digital trust: organisations could build a culture of privacy by maintaining high security standards, whilst also providing a positive user experience to further contribute to the exponential growth of the digital business market (Lindstrom and Rounds, 2018).

However, there are confusions regarding the legal frameworks of digital trust, and as a result, it is often argued that businesses cannot singlehandedly maintain digital trust without support from governance and policies.

Based on these arguments, we could propose that businesses and governments must work collectively to maintain privacy standards and to enhance data protection regulations in order to reap the benefits of a secure digital trust system. Nevertheless, as we have previously stated, privacy and security are not the only factors which promote digital trust: a recent report by Deloitte Insights has stated that digital trust can be hindered by a perception of loss of control (Albinson et al.). Hence, it could be argued that a solution to the digital trust debate is the wide-scale implementation of blockchain (Jamal et al., 2019).

Blockchain is an open-source technology which enables the transfer of digital information across a network without requiring verification from a third-party. This approach has been referred to as the “cornerstone of digital trust infrastructure” due to its enhanced security and incredibly transparent nature (Anon, 2021). Blockchain is decentralised, therefore it denies hackers a single point of attack, and it provides individuals with high levels of control by allowing them to review who has access to their data.

"User privacy and public safety can and should work in tandem" - Sen. Marsha Blackburn

How will the debate between access to encrypted data (or lack thereof) be solved in the future? Can it ever be solved?

"User privacy and public safety can and should work in tandem."

The above statement comes from Senator Marsha Blackburn (R-Tennessee), a drafter of the Lawful Access to Encrypted Data Act (2020). At face value, the statement is logical. However, after understanding the intricacies of encryption, the fundamental rights of individuals to privacy and freedom of expression, and the potential dangers of creating backdoors/key escrows to encrypted data for governments/law enforcement, one must ask themselves: is there a middle ground wherein safety can be guaranteed to individuals and private trust companies whilst governments/law enforcements have access? Who defines security, safety, and privacy – the individual, the private company, and/or government/law enforcement? Who’s definition should set the precedent? The answer to these questions may not come for a long while – or it may not come at all, due to the divisive nature of this debate.

Future considerations for digital trust/cyber security

It was found that most users were not aware of how their data was being used and did not feel in control of their own data. Users were also not aware of their rights and frameworks in place concerning their data and privacy. Companies are keen to pay for cybersecurity services as there is a shortage in professionals but a need to comply to Government regulations, and they also want to minimise losses from security breaches. Different cybersecurity use-cases require different business models, and cybersecurity companies must review regulations and external factors regularly in order to maintain their competitiveness in the market.

References

Abraham, C., Sims, R. R., Daultrey, S., Buff, A. & Fealy, A. (2019) How Digital Trust drives culture change. *MITSloan.* [Online] Available at: https://sloanreview.mit.edu/article/how-digital-trust-drives-culture-change/ [Accessed 22 July 2021]

Albinson, N., Balaji, S. & Chu, Y. 'Building digital trust: Technology can lead the way', *Deloitte Insights,* [online] Available at: *https://www2.deloitte.com/lu/en/pages/innovation/articles/building-long-term-trust-in-digital-technology.html* [Accessed 18 July 2021]

Anon (2019) 'Case Study 8: Estonia e-government and the creation of a comprehensive data infrastructure for public services and agriculture policies implementation', *Digital Opportunities for Better Agricultural Policies* [Online]. Paris: OECD Publishing. pp. 207–213.

Anon (2020) '*Is digital ID a good idea? Everything you need to know.'* Digital ID. [online] Available at: https://www.digitalid.co.uk/blog/is-digital-id-a-good-idea [Accessed 23 July 2021].

Anon (2021) *How to ensure Digital Trust in the world of Digitalisation* [Online] Available at: https://subex.medium.com/how-to-ensure-digital-trust-in-the-world-of-digitalization-d4025c7352df [Accessed 22 July 2021]

AppViewX (2021) *Public Key Infrastructure*, image, <https://www.appviewx.com/wp-content/uploads/2020/10/education-center-public-key-infrastructure.jpg> [Accessed 29 July 2021]

Aretiico Limited (2021) *About Us*. [Online] Available at: https://aretiico.com/about-us/ [Accessed 22 July 2021]

Baltimore Technologies plc (2002) *Baltimore UniCERT the world's leading PKI*. Available at: http://www.zolwik.eu/compl/data/betrusted/pdf/BaltimoreUniCERTProductBrochure.pdf [Accessed 22 July 2021]

Bar Am, J., Furstenthal, L., Jorge, F. & Roth, E. (2020) 'Innovation in a crisis: Why it is more critical than ever', *McKinsey & Company* [online] Available at: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/innovation-in-a-crisis-why-it-is-more-critical-than-ever [Accessed 20 July 2021]

Bhalla, A., Chakravorti, B. & Chaturvedi, R. S. (2021) *How Digital Trust Varies Around the World*. *Harvard Business Review* [Online] Available at: https://hbr.org/2021/02/how-digital-trust-varies-around-the-world [Accessed 21 July 2021]

Bissell, K., LaSalle, R. & Dal Cin, P. (2019) *Ninth Annual Cost of Cybercrime Study*. [Online] Available at: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study [Accessed 23 July 2021]

Bondar, M., Lee, J. & Weirens, J. (2021) New models for building digital trust: An interview with MIT's Sandy Pentland. *Deloitte Insights* [Online] Available at: https://www2.deloitte.com/uk/en/insights/digital-transformation/the-importance-of-digital-trust-qa.html [Accessed 20 July 2021]

Booth, A., Dhingra, A., Heiligtag, S., Nayfeh, M. & Wallance, D. (2020) *Critical infrastructure companies and the global cybersecurity threat*. Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf [Accessed 22 July 2021]

Briz, N. (2018) *This is Your Digital Fingerprint.* [Online] Available at: https://thedisconnect.co/two/your-digital-fingerprint/ [Accessed 13 July 2021]

CA Security Council (2016) *Leading Certificate Authorities and Microsoft Introduce New Standards to Protect Consumers Online*. [Online] Available at: https://pkic.org/2016/12/08/leading-certificate-authorities-and-microsoft-introduce-new-standards-to-protect-consumers-online/ [Accessed 22 July 2021]

Cater, L. (2021) What Estonia's digital ID scheme can teach Europe. *Politico*. [Online] Available at: https://www.politico.eu/article/estonia-digital-id-scheme-europe/ [Accessed 22 July 2021]

Channel 4 (2021) *Your Data.* [Online] Available at: https://www.channel4.com/4viewers/your-data [Accessed 19 July 2021]

Committee of the Judiciary (2020) *Graham, Cotton, Blackburn Introduce Balanced Solution to Bolster National Security, End Use of Warrant-Proof Encryption that Shields Criminal Activity* [Online]. Available at: https://www.judiciary.senate.gov/press/rep/releases/graham-cotton-blackburn-introduce-balanced-solution-to-bolster-national-security-end-use-of-warrant-proof-encryption-that-shields-criminal-activity [Accessed 18 July 2021]

Covey, S. M. R. and Merrill, R. R. (2018) *The Speed of Trust: the one thing that changes everything*. New York: Free Press.

Cracknell, R., Kaplan, J., Richter, W., Shenton, L. & Stewart, C. (2020) *Securing software as a service*. Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cybersecurity%20in%20a%20digital%20era/Cybersecurity%20in%20a%20Digital%20Era.pdf [Accessed 22 July 2021]

Day, M. (2021) *How Do Cybersecurity Companies Make Money?* [Online] Available at: https://startacybercareer.com/how-do-cybersecurity-companies-make-money/ [Accessed 22 July 2021]

ENISA (2018) *The Value of Personal Online Data*. [Online] Available at: https://www.enisa.europa.eu/publications/info-notes/the-value-of-personal-online-data [Accessed 12 July 2021]

Espinoza, A.M., Tolley, W.J., Crandall, J.R., Hilts, A.S., & Crete-Nishihata, M. (2017). 'Alice and Bob, who the FOCI are they?: Analysis of end-to-end encryption in the LINE messaging application', *FOCI*, 7 [online]. Available at: https://www.usenix.org/system/files/conference/foci17/foci17-paper-espinoza.pdf [Accessed 21 July 2021]

Etzioni, A. (2014) The Private Sector: A reluctant Partner in Cybersecurity. *Georgetown Journal of International Affairs*, 69-78. Available at: http://www.jstor.org/stable/43773650 [Accessed 18 July 2021]

European Union Working Party 29. (2018) Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU. Brussels. European Union.

Forward Business and Intelligence Co., Ltd. (2014) *2015年中国信息安全分析行业发展前景浅析*. [Online] Available at: https://bg.qianzhan.com/report/detail/361/141212-9439d8c4.html [Accessed 19 July 2021]

Gartner, 2021. Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. [Online] Available at: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem [Accessed 28 July 2021].

Gomes, J. F., Iivari, M., Ahokangas, P., Isotalo, L., & Niemela, R. (2017) Cybersecurity Business Models for IoT-Mobile Device Management Services in Futures Digital Hopsitals. *Journal of ICT Standardization*, 5 (6), 107-108. Available at: https://www.riverpublishers.com/journal_read_html_article.php?j=JICTS/5/1/6 [Accessed 22 July 2021]

Gomes, J. F., Iivari, M., Ahokangas, P., Isotalo, L., Sahlin, B. & Melén, J. (2018) Cyber Security Business models in 5G. *A Comprehensive Guide to 5G Security*, pp. 99-116. Available at:

https://www.researchgate.net/publication/322466981_Cyber_Security_Business_Models_in_5G [Accessed 23 July 2021]

Goodell, G. & Aste, T. (2019) 'A Decentralised Digital Identity Architecture', *Frontiers in Blockchain.*

Grand View Research (2021) *Cyber Security Market Size, Share & Trends Analysis Report By Component, By Secruity Type, By Services, By Deployment, By Organization, By Application, By Region, And Segment Forecasts, 2021 – 2028*. [Online] Available at: https://www.grandviewresearch.com/industry-analysis/cyber-security-market [Accessed 18 July 2021]

Huang C. C. & Yuan Z. (2020) 'Privacy Implication and Technical Requirements Toward GDPR Compliance'. In: Arai K., Bhatia R., Kapoor S. (eds) *Proceedings of the Future Technologies Conference. FTC 2019. Advances in Intelligent Systems and Computing*. https://doi-org.libproxy.ncl.ac.uk/10.1007/978-3-030-32523-7_24

Humby, C. (2006) 'Data is the new Oil!', *ANA Senior marketer's summit*, Kellogg School. Available at : http://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Jackob, M. (2001) 'History of Encryption', *SANS Institute* [online]. Available at: https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [Accessed 18 July 2021]

Jamal, A., Helmi, R. A. A., Syahirah A. S. N. & Fatima, M.(2019) Blockchain-Based Identity Verification System. *IEEE 9th International Conference on System Engineering and Technology (ICSET)*. [Online] Available at: https://ieeexplore-ieee-org.libproxy.ncl.ac.uk/document/8906403 [Accessed 23 July 2021]

Kan, M. (2017) *WannaCry Ransomware*, image, CSOonline.com <https://images.techhive.com/images/article/2017/05/img_20170515_140831_01-100722789-large.jpg> [Accessed 29 July 2021]

Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Geneva: United Nations Human Rights Council.

Kircheimer, S. (2013) *Cybercrime Costs 508,000 U.S. Jobs*. Available at: http://blog.aarp.org/2013/07/25/cybercrime-costs-508000-u-s-jobs/ [Accessed 18 July 2021]

Lindstrom, P. & Rounds, M. (2018) 'Digital Trust: The Key Driver for Digital Transformation', *IDC.* [online] Available at:

https://www.idc.com/getdoc.jsp?containerId=US43986218 [Accessed 19 July 2021]

Linus, R. (n.d.) *What every Browser knows about you.* [Online] Available at: https://webkay.robinlinus.com/ [Accessed 13 July 2021]

Ludin, J. (2021) *"Public Key Infrastructure: Explained." SecureW2* [Online] Available at: https://www.securew2.com/blog/public-key-infrastructure-explained [Accessed 12 July 2021]

Malwarebytes (2019) *The Blinding Effect of Security Hubris.* [Online] Available at: https://www.malwarebytes.com/resources/files/2019/03/190226-mwb-security-hubris-on-data-privacy-v2.pdf [Accessed 17 July 2021]

Mazhar, F., Rizwan, M., Fiaz, U., Ishrat, S., Razzaq, M.S., & Khan, T.N. (2014) An Investigation of Factors Affecting Usage and Adoption of Internet & Mobile Banking In Pakistan. *International Journal of Accounting and Financial Reporting*, 4(2), http://dx.doi.org/10.5296/ijafr.v4i2.6586 [Accessed 24 July 2021]

McNicholas, E. & Angle, K. (2020) *USA: Cybersecurity Laws and Regulations 2021*. [Online] Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa [Accessed 23 July 2021]

Miliefsky, G. (2014) *Flashlight Apps Threat Assessment Report.* [Online] Available at: http://web.archive.org/web/20141218095121/http://www.snoopwall.com/wp-content/uploads/2014/10/Flashlight-Spyware-Appendix-2014.pdf [Accessed 18 July 2021].

Morey, T., Forbath, T. & Schoop, A. (2015) Customer Data: Designing for Transparency and Trust. *Harvard Business Review,* pp. 96-105.

Network Encyclopedia (2021) *Cloud Computing*, image, <https://networkencyclopedia.com/wp-content/uploads/2019/09/cloud-computing.png?ezimgfmt=ng:webp/ngcb2> [Accessed 29 July 2021]

Nohe, P. (2020) *Why the Lawful Access to Encrypted Data Act is a Threat to Your Rights and Privacy* [Online]. Available at: https://www.globalsign.com/en/blog/why-lawful-access-encrypted-data-act-threat-your-rights-and-privacy [Accessed 22 July 2021]

Olsen, M., Schneier, B., & Zittrain, J. (2016) *Don't Panic: Making Progress on the Going Dark Debate* [Online]. Available at: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [Access 21 July 2021]

O'Neill, O. (2020) Trust and Accountability in a Digital Age. *Philosophy*. Cambridge University Press, 95(1), pp. 3–17. doi: 10.1017/S0031819119000457.

Okta (2021) *The State of Digital Trust*. [Online] Available at: https://www.okta.com/the-state-of-digital-trust/ [Accessed 12 July 2021]

Paleofuture (2019) *The ARPA Network August 1972*, image, <https://images.squarespace-cdn.com/content/v1/5c647bc99b7d150fe925ea5c/1551203068518-ET7K8P9B5ETYRWAOESDE/18urgu85a743fjpg.jpg?format=2500w> [Accessed 29 July 2021]

Pandora (2021) *Pandora Privacy Policy.* [Online] Available at: https://www.pandora.com/privacy [Accessed 19 July 2021]

Parsons, C. (2019) *Canada's New and Irresponsible Encryption Policy: How the Government of Canada's New Policy Threatens Charter Rights, Cybersecurity, Economic Growth, and Foreign Policy* [Online]. Available at: https://citizenlab.ca/2019/08/canadas-new-and-irresponsible-encryption-policy-how-the-government-of-canadas-new-policy-threatens-charter-rights-cybersecurity-economic-growth-and-foreign-policy/ [Accessed 18 July 2021]

Pew Research Center (2019) *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* [Online] Available at: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information [Accessed 15 July 2021]

Pinkham, J. (2019) What's the Best Way to Build Digital Trust? Show your customers you care about their privacy. *Security Intelligence* [Online] Available at: https://securityintelligence.com/posts/whats-the-best-way-to-build-digital-trust-show-your-customers-you-care-about-their-privacy [Accessed 19 July 2021]

PKI Consortium (2021) *About the PKI Consortium*. [Online] Available at: https://pkic.org/about/ [Accessed 22 July 2021]

Prinsley, M., Yaros, O., Vanryckeghem, V., Randall, R. & Hajda, O. (2021) *UK Government announces plans for new cybersecurity legislation to protect consumer smart devices*. [Online] Available at: https://www.mayerbrown.com/en/perspectives-events/publications/2021/04/uk-government-announces-plans-for-new-cybersecurity-legislation-to-protect-consumer-smart-devices [Accessed 22 July 2021]

P&S Intelligence (2021) *Digital Signature Market To Generate Over $25,211.3 Million Revenue by 2030 Says P&S Intelligence*. Available at: https://www.bloomberg.com/press-releases/2021-06-28/digital-signature-market-to-generate-over-25-211-3-million-revenue-by-2030-says-p-s-intelligence

Ragnedda M. (2020) Theorizing Inequalities. In: Enhancing Digital Equity. Palgrave Macmillan, Cham. https://doi-org.proxy.library.cornell.edu/10.1007/978-3-030-49079-9_2

Reference for Business (2002) *Baltimore Technologies Plc – Company Profile, Information, Business Description, History, Background Information on Baltimore Technologies Plc*. [Online] Available at: https://www.referenceforbusiness.com/history2/52/Baltimore-Technologies-Plc.html [Accessed 22 July 2021]

Satpathy, T. (2017) 'The Aadhaar: "Evil" Embodied as Law', *Health Technol (*7), pp. 469–487. Available at: https://doi.org/10.1007/s12553-017-0203-5

Shanghai Laoqin Information Technology Co., Ltd. (2019) 智联招聘发布《网络安全人才市场状况研究报告》[Online] Available at: http://www.coho.com.cn/Journalism01?article_id=423&pagenum=1 [Accessed 19 July 2021]

Slaymaker, S. (2020) The Importance of Establishing Digital Trust. *No Jitter*. Available at: https://www.nojitter.com/unified-communications-collaboration/importance-establishing-digital-trust [Accessed 12 July 2021]

Statista (2021) *Annual number of data breaches and exposed records in the United States from 2005 to 2020.* [Online] Available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [Accessed 12 July 2021]

Svilar, A. and Zupančič, J. (2016) User Experience with Security Elements in Internet and Mobile Banking. *Organizacija*, Vol.49 (Issue 4), pp. 251-260. https://doi.org/10.1515/orga-2016-0022

Swiss Cyber Forum (2020) *Cyber Security Statistics 2020*, image, Swiss Cyber Foundation <https://www.swisscyberforum.com/blog/cyber-security-statistics-2020-infographic/> [Accessed 29 July 2021]

Szoldra, P. (2016) *This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks* [Online]. Available at: https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [Accessed 22 July 2021]

The Associated Press (2016) *FBI breaks into iPhone of San Bernardino shooter without Apple's help*. [Online] Available at: https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [Accessed 22 July 2021]

Thomson, S. (2019) '*We're closer to the knife's edge': Confrontation looming on encryption 'backdoors' as Goodale looks for balance* [Online]. Available at: https://nationalpost.com/news/politics/were-closer-to-the-knifes-edge-confrontation-looming-on-encryption-backdoors-as-goodale-looks-for-balance [Accessed 20 July 2021]

Ting, H. L. J., Li, X. K. T., Wang, H. & Chu, C. (2021) *On the Trust and Trust Modelling for the Future Fully-Connected Digital World: A Comprehensive Study*. [Online] Available at: https://search-ebscohost-com.proxy.library.cornell.edu/login.aspx?direct=true&db=edsarx&AN=edsarx.2106.07528&site=eds-live&scope=site [Accessed 12 July 2021]

Tsakanyan, V. T. (2017) The role of cybersecurity in world politics. Vestnik RUDN. International Relations, 17(2), 339—348

United Kingdom's Attorney General's Office and Home Affairs. (2019) Joint Meeting of the Five Country Ministerial and quintet of Attorney's General: communique. London. Government of the United Kingdom.

VanDerWerff, E. & B. Lee, T., 2015. The 2014 Sony hacks, explained. [Online] Available at: https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea [Accessed 7 July 2021].

White, O., Madgavkar, A., Manyika, J., Mahajan, D., Bughin, J., McCarthy, M. & Sperling, O. (2019) 'Digital identification: A key to inclusive growth', *McKinsey Digital* [online] Available at: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx [Accessed 20 July 2021]

Wikipedia (n.d.) *Internet users in 2015 as a percentage of a country's population*, image, Wikimedia Commons, <https://upload.wikimedia.org/wikipedia/commons/thumb/9/99/InternetPenetrationWorldMap.svg/700px-InternetPenetrationWorldMap.svg.png> [Accessed 29 July 2021]

Zucker, L. G. (1986) The Production of Trust: Institutional Sources of Economic Structure, *Research in Organizational Behaviour*, pp. 53-111.