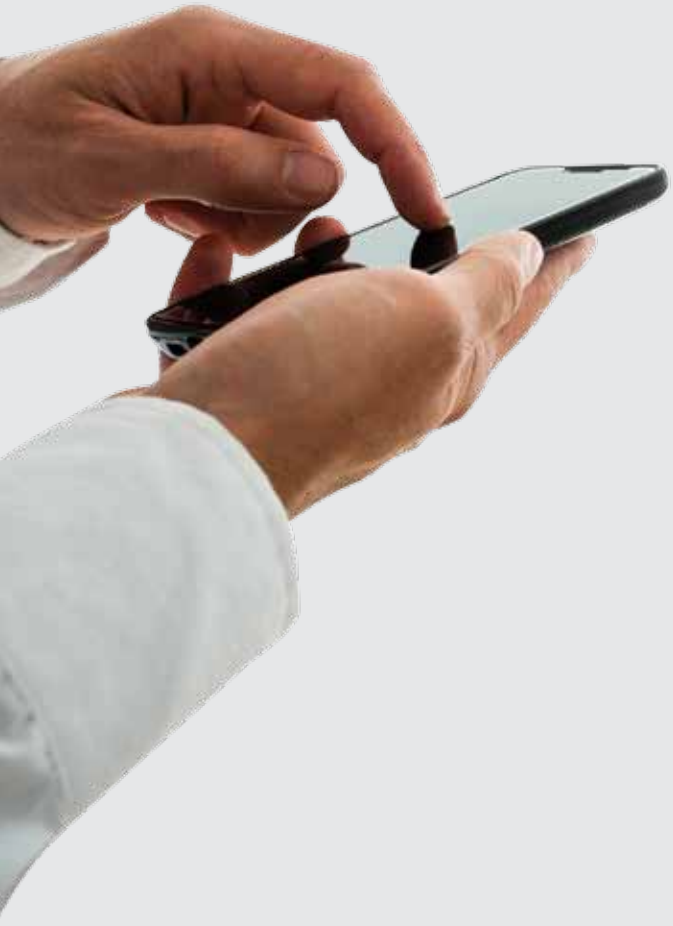
Management Summary

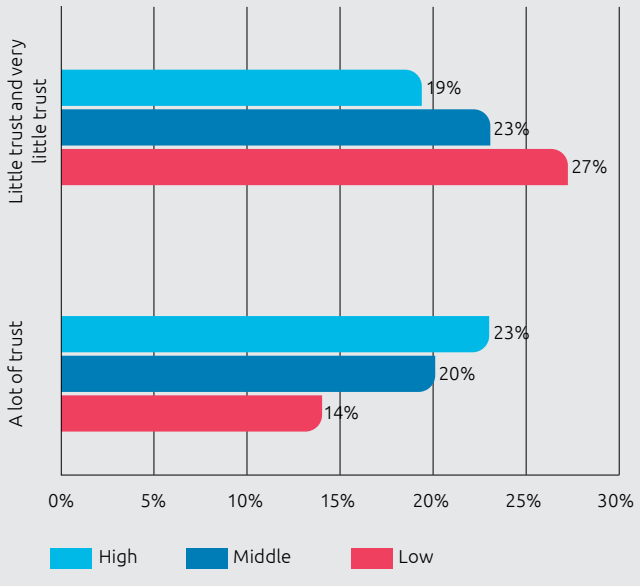
(Dis)trust in the digital society

The digital society is based on trust. We rely upon governments and organizations to treat data with integrity and care, and we trust that personal information will not be laid bare for everyone to see. We trust that information we receive can be treated as facts and that the truth is not manipulated.



At least, that used to be the case. Since then, we have wised up to reality and found that our trust was unwarranted all along. For a long time we did not know what could happen if effective security measures are lacking, or if people with sinister motives hijack our data. On top of that, we were unaware of the risks of installing new apps on our devices. The digital society had no precedent; we had no previous experience with its downsides.

Figure 1 : Trust in the digital society is divided (based on educational level).



Rude awakening

Recent developments have led to a rude awakening. We have found out that public and private organizations gather data, often for unclear and disputable ends. Our personal data are less secure than we thought, as a result of ineffective authentication processes. We have experienced the potentially enormous fallout of hacks. And even parties we entrusted our data to, believing their claims of vault like security, turn out to be vulnerable to security breaches. Large scale migration of data to the cloud has resulted in a potentially enormous information leak. Through our widespread use of social media, we have created a gold mine of data that, again, is far less secure than we would like. Thanks to Cambridge Analytica, the daily Facebook-adventures of 80 million people were left out on the street – facilitated, incidentally, by Facebook's convoluted privacy settings.

And that's not all. The intimate knowledge that many organizations have about us, leaves us vulnerable to manipulation. The aforementioned Cambridge Analytica used Facebook data to influence the American presidential elections. Fake news – discussed in chapters 3 and 12 of this report – falls on fertile ground. We all live in an online bubble of our own making, facilitated by smart algorithms from Google and others. This leaves us vulnerable to manipulation and susceptible towards one sided versions of the truth.

The unprecedented outpouring of new technologies – Internet of Things, robotization, artificial intelligence – represents a further challenge to our cyber security. The digital resilience of people and organizations cannot keep up with the developments; the wolves at the door have the upper hand. Our lack of expertise and lack of knowledge cause significant holes in our defences, and criminal elements have no compunctions at all about exploiting them.

The digital society, then, is increasingly founded upon quick sand. We have woken up to digital reality. A reality we are not comfortable with.

Figure 2: 1 out of the 10 persons never changes his password

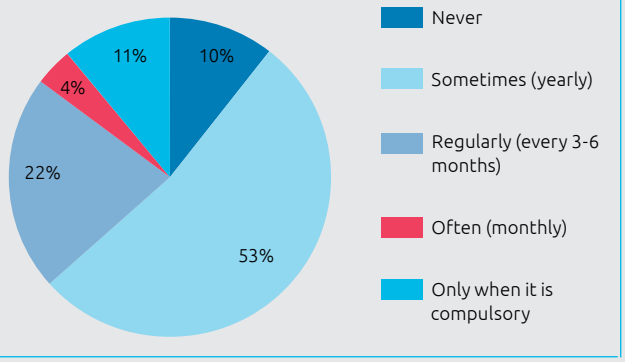
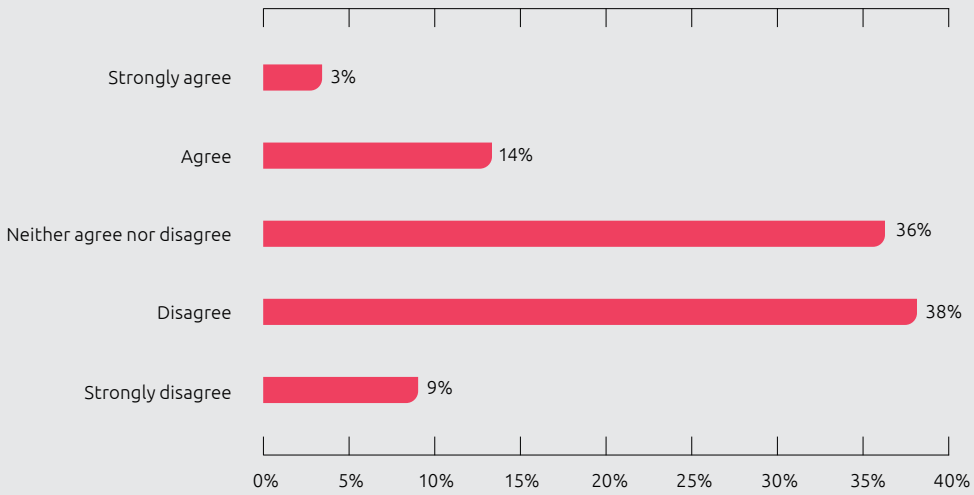


Figure 3: Compared to 5 years ago, 47% encounters less distinction between true and false facts.



> *More and more it turns out that the digital society is built on quicksand. We have woken up in a digital reality. And we are not that fond of it.*
>
> **Erik Hoorweg**
> **Capgemini Consulting**

Tipping point

This leaves us at a tipping point. The point where trust is about to turn into distrust. We are turning our backs on Facebook. In the Netherlands, we have voted against the Wiv-referendum (Intelligence and Security Services Act). We are losing faith in the media, the government and the private sector. The growing role of artificial intelligence is mostly regarded with suspicion.

Now that citizens are becoming aware of the risks, digital society is under threat. What will happen if citizens revoke their consent? If they no longer concur to organizations' access to their data? Modern business models in private and public sector rely on this (personal) data. Without consent, the whole system folds like a house of cards.

There is another factor at play. As chapters 4 and 9 of this report argue, our personal and national security rely on our ability to gather, share and analyze data. This seems to run contrary to our notion of privacy. However: privacy is a human right, but safety is a precondition for our ability to enjoy it. The trick, then, is in striking the right balance between these two themes.

Opportunity

Institutions in the security domain have become more aware of the part they have to play in rebuilding trust and reaffirming our security and safety. This has already resulted in several measures.

The Dutch government, for instance, has adopted the General Data Protection Regulation (GDPR). This EU measure aims to improve the protection of citizens' privacy and establishes stricter technical and organizational rules for the gathering of data by organizations. It also prescribes supplementary rules and regulations about data handling by intelligence services. Moreover, we see that measures are being taken – in Germany for instance - to counter fake news, through judicious use of

Figure 4: Just 9% does not feel comfortable with cameras in public areas.

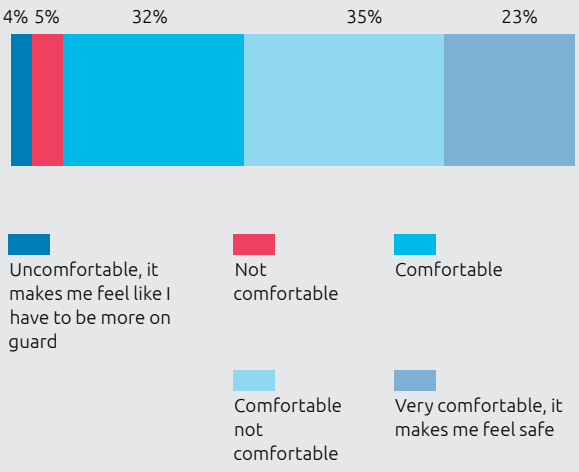
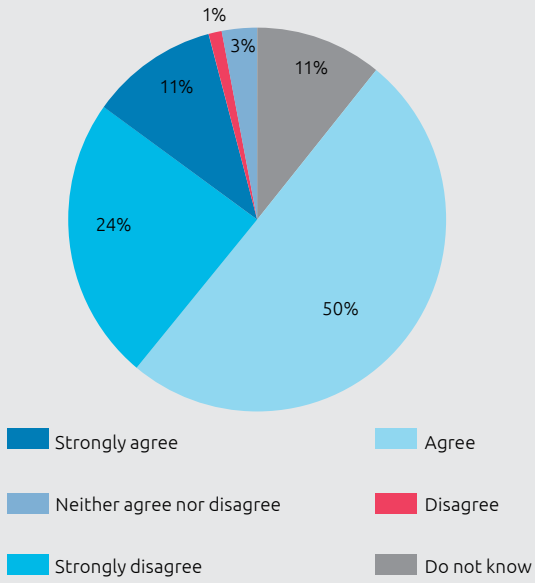


Figure 5: 61% is concerned about the security of IoT devices



> *It should be clear: there is role to play for everyone in the security domain when it comes to improving data protection and increasing digital security. Taking that responsibility seriously is the first step towards rebuilding the damaged trust of people.*
>
> **Erik Hoorweg**
> **Capgemini Consulting**

smart algorithms. Finally, the war against cybercrime and cyber threats from abroad is gaining momentum. The Dutch Justice minister Grapperhaus has called it a top priority of the new cabinet, rolled out in explicit international collaboration with governments and the private sector. Incidentally, The Netherlands was already at the forefront of the cyber security effort.

Institutions in the security domain will have to regard such measures as an opportunity. An opportunity to clean house, for instance. New regulations demand that organizations offer insight into their data environment; a transparency that is often lacking. A restructuring and rationalization of the application landscape, then, will be necessary. This also benefits the organizations themselves.

There is more. When introducing and developing new products and services, organizations will have to – from the onset! – consider the security aspect. The potential impact of any product or service for citizens' security should always be top of mind.

Everyone in the security domain has a part to play in the improvement of data protection and digital security. If we take this responsibility seriously, we have taken an important first step towards rebuilding the citizen's trust.

Good and evil

Technology can be used for different purposes. Good and evil. Recently, evil seemed to have gained the upper hand. All the parties involved now have a responsibility to fight the good fight. To use often disruptive technology to promote security, while respecting the privacy of individuals. To search for the human dimension in technology. To not leave citizens to their own devices, but offer guidance in a digital world. To enter into partnerships with those citizens and to give shape to citizens' role as participants. To build and safeguard the trust in - and reliability of – digital developments. And to, within that context, strive towards safety and security for all of us.

We hope you enjoy reading Trends in Security 2018.

About the author:

Drs. Erik Hoorweg MCM is vice president at Capgemini Consulting and responsible for the public sector.

For more information you can contact the author via:

erik.hoorweg@capgemini.com |

https://www.linkedin.com/in/erik-hoorweg-296b593/

The data in the report is based upon GFK's survey (N=1000, December 2017), conducted on behalf of Capgemini Nederland B.V.