Capgemini

Trends in Cybersecurity 2018

(Dis)trust in the digital society

Preface

Digital developments provide a connected society. Internet connects people, organizations, and devices on a large scale. Think, for instance, of biometrics and the Internet of Things (IoT). This brings along unprecedented opportunities. It will not be long before everyone and everything is permanently connected to the internet. It is obvious that far-reaching digitization will radically change almost every aspect of society, not only in the Netherlands but worldwide. Humanity is becoming more and more dependent on technology every day. The central question to this Trends in Cybersecurity edition is therefore; “Can we rely on the digitization of our society?”

Distrust in rules and developments

Digitization is a hot issue. Since May 25th, 2018, companies and organizations are obliged to work in compliance with the GDPR legislation and have set up their processes accordingly. Although many organizations see this as a necessary evil, it could also offer great opportunities for a thorough review of privacy, data processing, and data storage. Previously, data was only used as a source, current developments however enable us to make predictions based on data. Predictive policing, for example, already enables us to predict where to expect turmoil or crime.

Big data is not just a concept that is used by experts. Digitization is now part of the society. This is also evident from the results of the referendum regarding the Wiv (Intelligence and Security Services Act in the Netherlands). Until recently this used to be a topic only techies or politicians had an opinion about but today everybody has become an “expert”. And perhaps it is good to be critical about how the government and organizations deal with our (personal) information.

Gain trust

The challenge lies in using data properly, for example to fight terror or crime, without harming civilian trust. Unfortunately, technological developments have clearly demonstrated their negative aspects as well (e.g. troll accounts, fake news, hacks, and phishing emails). That is why it is of the utmost importance to further develop and improve ways of access authentication in order to maintain a secure society and (re)gain confidence in technology. Biometrics could play a major role in this. Another way to secure our data is Universal 2-factor authentication.

With the rise of smartphones and other products for private use, the digital world has become more and more accessible to everyone. In addition to the threats mentioned earlier, this offers enormous opportunities. The police, for example, have developed apps that encourage citizen participation and that are used to help find missing people or cars. Currently, everything can be recorded through dashcams, mobile or private cameras, and live connections with control rooms. Security provided by just the government is surely over.

The emerging digitization raises drastic dilemmas, challenges, and opportunities throughout society. Technological developments could open the door to greater prosperity, health, well-being, security and sustainability – but only if we ensure that new technology, people and societies enhance each other.

Successful digital transformation requires digital vision, leadership and digital capabilities. In this edition of Trends in Cybersecurity you will come across familiar examples. Do you trust or distrust these new trends?

We hope that this report helps to outline a vision for the future and gives you concrete tools for short term use.

Enjoy reading!

On behalf of Capgemini Nederland B.V.
and Capgemini Invent

Erik Hoorweg and Paul Visser

Trends in Cybersecurity 2018

Contents

Preface

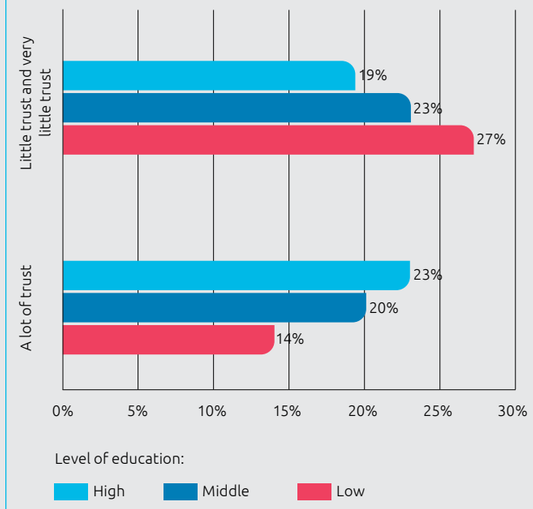
Management Summary

(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 - topic of some articles in 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 cybersecurity. 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 quicksand. 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 or her password.

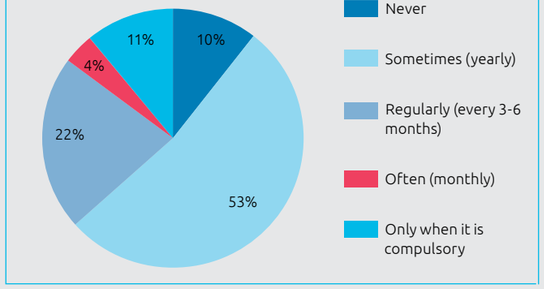
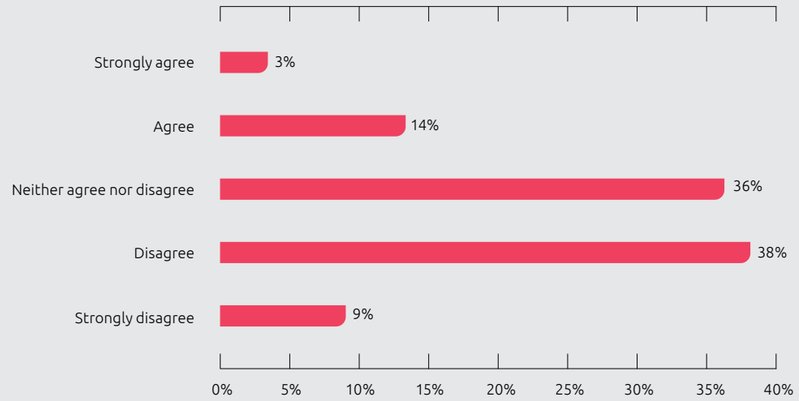


Figure 3: Compared to 5 years ago, 47% encounters less distinction between true and false facts.



> *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 Invent**

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 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 cybersecurity effort.

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

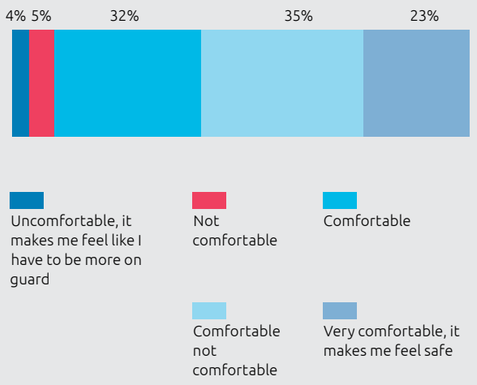
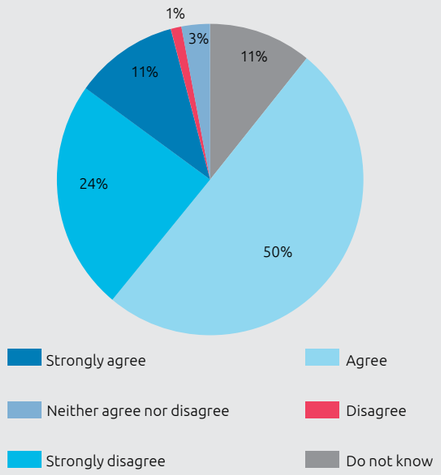


Figure 5: 61% is concerned about the security of IoT devices.



> *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 Invent**

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 Invent and responsible for the public sector.

For more information you can contact the author via:

erik.hoorweg@capgemini.com

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

Fake news: a double threat

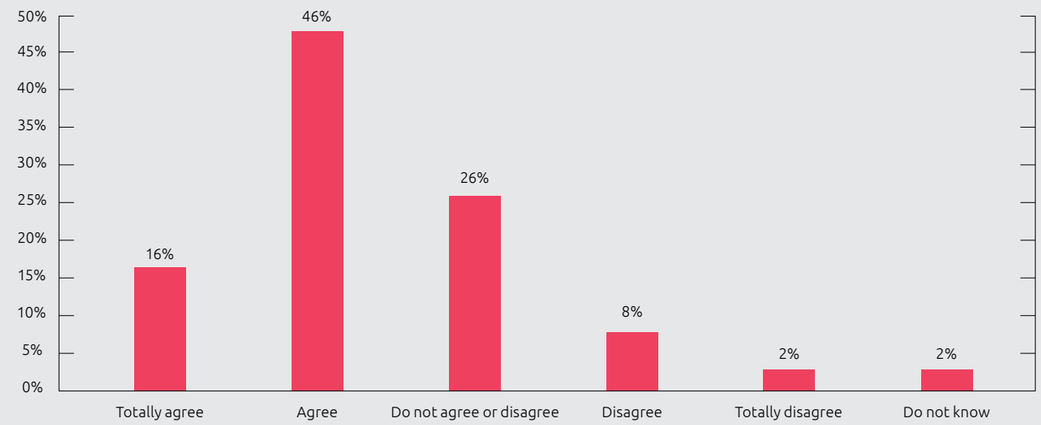
How does fake news pose a double threat to national security in the Netherlands and how can we stand against it?

The spread of fake news is much debated. Civilians worry. Intelligence services struggle to detect and oppose the spread of fake news. GfK[1] research shows that 62% of civilians regard the spread of fake news as a threat to their own security as well as a threat to society in general. How do you separate opinion from inaccurate information and how do you make sure that measures taken against fake news do not result in censorship.

Highlights

- **Intentional spread of fake news is not new.**
- **New dynamics due to social media and the internet.**
- **Disinformation poses a double threat to national security**
- **Disinformation jeopardizes vital interests of our state and/or society and disrupts our community.**
- **Be aware! Don't let precautions against disinformation become a threat as well!**

I preceive the spread of fake news as a threat to the safety of myself or of society.



For years states have been trying to influence each other by spreading unilateral or manipulated information. Unlike what the media wants us to believe the intentional spread of fake news is not a new phenomenon. Think, for instance, about propaganda and censorship that have been used in various dictatorships. What is new, however, is the way this information is being spread: via the internet and, especially, through social media. One of the many examples is the launch of a fake Dutch government website that contained inaccurate information but was not recognizable as such. The internet and the ever-increasing use of social media creates new dynamics when it comes to the way information, and also fake news, is spread: wide distribution is easy, anonymous and cheap.

There is much to do about fake news in Dutch media and politics, especially when it comes to alleged fake news from Russia. In November 2017, Sybrand Buma (of the Christian Democratic Party) noted that these Russian activities "could possibly be one of the greatest threats to our democracy"[2]. Minister Ollongren of Internal Affairs also warned the House of Representatives against the increased spread of disinformation coming from Russia[3]. Rob Bertholee, director-general at the General Intelligence and Security Service (AIVD) classifies Russia as "exceptionally active". He mentions that the spread of fake news by Russia is plentiful, even when there aren't elections. "Russia has been attempting to this daily, for a significant amount of time now. It's not new to us". Apart from Russia Betholee also mentions China and Iran as countries that wage digital war on Dutch targets[4].

To explain why the spread of fake news from states like Russia poses a threat to the stability and security of the Dutch society this article will elaborate on what fake news actually is, why it poses a threat and what we can do to stand against it. By taking precautions against the spread of fake news we must be aware of the rise of a new, unintended threat: censorship.

[1] GfK Research on "the Dutch", commissioned by Capgemini Nederland B.V. December 2018 (http://denieuwedraai.nl/hudson-yards-is-de-eerste-quantified-community-ter-wereld/)

[2] https://www.tweedekamer.nl/nieuws/kamernieuws/debat-over-regeringsverklaring-kabinet-rutte-iii

[3] https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2017Z15286&did=2017D32153

[4] https://trlnieuws.nl/nederland/politiek/aivd-rusland-probeerde-met-nepnieuws-onze-verkiezingen-te-beinvloeden

Fake news

Bluntly said: fake news consists of lies wrapped up to look like news. But fake news is also our interpretation of reality, a divide-and-conquer strategy and the intentional spread of disinformation. In the media fake news is a catch-all concept for bad journalism, political framing, propaganda, misleading ads and a means to an end for states to achieve their (economic and political) goals.

To point out the true meaning of fake news scientist argue to use the following definition when it comes to disinformation: the deliberate spread of incorrect information with the aim of harming individuals, socials groups, organizations or countries[5]. To the purpose of this article we will keep to this definition because deliberate spread of disinformation by states is regarded as covert political manipulation[6]. Disinformation is mostly made up out of imputations. The main goal, even more than just misinforming, is to polarize and destabilize. Disinformation is usually not recognizable as such and is often believed as being true. This believe consequently leads to undermine trust between civilians and politicians, civilians and the media and even civilians amongst themselves. It amplifies divergencies that exist in any democracy or evokes divergencies that were not present before. Western democracies fear the use of disinformation by potential rivals to expand their power and influence in other countries[7].

That these covert affairs are actually happening is evident from the spread of disinformation by a "fake news fabric" in St. Petersburg. They distributed disinformation at the time of the U.S. presidential elections and also about the Ukraine-EU association agreement referendum. They did the same in the MH17 investigation and at the Brexit referendum. Chances of getting in contact with disinformation grow because of the online availability. We no longer need to go and find information that confirms what we think to be true on our own. Algorithms now find it and display it to us. These algorithms define for the most part what it is that we believe. If we are mainly focused on news about the refugee crisis then we will get mainly notifications on our timeline about refugees. This brings about islands of information and people tend to create tunnel vision. This is also the case when it comes to disinformation. If people get involved in disinformation they will quickly find confirmation of this disinformation.

Double threat

To fully understand why the spread of disinformation poses a double threat to national security it's important to clarify the meaning of the concepts threat and security. The realm of defense establishes several forms of threat. The spread if disinformation to misinform, polarize and destabilize by means of covert manipulations is categorized as "subversion". Subversion is the openly spread of tendentious information, bring about damage of reputation and covert manipulation. In this way disinformation harms national security because it jeopardizes vital interests of our state and/or society and disrupts our community[8]. This is what we call the primary threat of disinformation.

The Dutch government acknowledges the dangers that come along with this primary threat and there are some initiatives that try to tackle it. Facebook has been working together with Nu.nl and Leiden University to detect fake news and prevent its spread. On European level there's an expert group at work that collects examples of fake news and brings them together in an online database. Critics however point out that their examples are often incorrect. If disinformation is detected and classified as such, it is then possible to eliminate it without engaging in censorship? This is where we come to the secondary threat of disinformation. It's a fine line between opinion and disinformation. Because of this fine line it's difficult to eliminate information or classify it as disinformation in a free democracy. This goes against freedom of speech at the one hand and raises the question of what authority is able to judge this objectively[9] on the other. Freedom of speech is one of the most fundamental cornerstones of our democracy. So, it is of utmost importance to cope carefully with this blurry line between opinion and disinformation. The Netherlands must be careful not to fight one evil (the spread of disinformation) with another (engaging in censorship).

The spread of disinformation will continue. As history shows, countries will keep on using (the spread of) disinformation as a way to covertly manipulate politics elsewhere. We live in an information driven society and technological possibilities are endless. Two years ago, Adobe presented software that analyzes someone's voice and then uses this same voice to say whatever you enter into the computer. Amazing technology which unfortunately could also be (mis)used by malicious minds. Because the distribution of disinformation will continue to grow and take on more innovative forms, it will be increasingly difficult for intelligence services to counteract them. Dick Schoof (National Coordinator for Security and Counterterrorism) says in an interview with Radio 1 that intelligence services are trying to monitor and detect disinformation, but it proves to be very difficult to do so. "It's not only getting more difficult to determine what is, or isn't, disinformation, but to uncover the source turns out to be tricky business as well[10]".

Battleground of the future

The development of fake news and the spread of disinformation threatens the national security of the Netherlands and has to be taken seriously. Disinformation can have profound effects on the way the Dutch society functions and on the social and political stability. To prevent being overrun by disinformation the focus needs to be on how to tackle the spread of fake news, both on societal and political level. This will not be an easy task for precautions taken against disinformation may just lead to a new threat: censorship.

The blurry line between opinion and disinformation makes it difficult to fight fake news in a democracy. However, this is the battleground of the future. The debate needs to become political and the government needs to support initiatives that counter the spread of disinformation. Civilians must learn to be critical regarding news in order to be able to recognize fake news. The media could be of great importance. Besides being mindful and alert they are able to develop procedures to keep each other focused and point out joint responsibility to tackle disinformation. It's up to intelligence and security services to invest in research and find ways to detect and expose disinformation. Finally, it's up to the Netherlands to be aware that precautions taken against disinformation do not become a threat to our democracy. If they do, we'll become pawns to the distributors of disinformation and we will still lose!

[5] **Council of Europe report DGI (2017)09**
[6] **AIVD annual report**
[7] **https://www.trouw.nl/democratie/europese-vrees-voor-russisch-nepnieuws-groeit~afe3898f/**
[8] **https://nctc.nl/binaries/strategie-nationale-veiligheid-2007_tcm31-32502.pdf**
[9] **htpps://elsevierweekblad.nl/buitenland/achtergrond/2018/01/eu-nepnieuws-577605/**
[10] **https://www.nporadio1.nl/dit-i-s-de-dag/onderwerpen/433645-dick-schoof-nederlanders-voelen-zich-veiliger**

About the authors:

Arieke van Os is a criminologist and senior consultant at Capgemini. She's active in the public and security domain and focuses on intelligence related issues.

Frits Broekema is principal consultant at Capgemini, active in the defense domain and focused on intelligence and security.

For more information you can contact the authors via:

arieke.van.os@capgemini.com

frits.broekema@capgemini.com

Mind the Gap!

How to close the gap between digital resilience and digital threat?

Highlights

- **The digital resilience of the Netherlands lags behind as digital threats increase, the gap is expanding.**
- **To close the gap we need a progressive approach on implementing innovations safely.**
- **Boardroom knowledge of cybersecurity is crucial in doing so.**

On June 21, 2017, Secretary of State Dijkhoff presented the Cyber Security Assessment Netherlands 2017[1] to the House of Representatives. The focus point was that the digital resilience of the Netherlands lags behind as digital threats continue to increase. Developments in information and communication technology (ICT) are moving extremely fast which results in an increasing threat by states and criminals. Our resilience, that consist of technological, organizational and people-orientated measures, can't keep up with these fast developments. The lack of cybersecurity results in a vulnerable society. The Cyber Security Assessment Netherlands 2018 states that the scope and severity of digital threats facing the Netherlands are still considerable and continue to evolve. The gap between resilience and threats keeps increasing. How do we get a hold on this?

Threat manifestation

On June 27, 2017 it became painfully clear how significant the impact can be when there was a worldwide ransomware contamination that also affected multiple Dutch organizations. The Petya malware (also known as WannaCry) crippled information supply of several organizations. Most notable was the stagnation in a container terminal. As a result of that stagnation all other logistic chains that were connected to it were profoundly disrupted as well. Numerous other organizations suffered tremendously as well, some for weeks at end, without the press publishing about this.

Increasing dependency

This cyberattack illustrates how, as a society, we greatly depend on accurately functioning ICT systems. When, as a result of a cyberattack, ICT systems fail to function correctly organizations and the chains in which they operate come to a halt. The dependency on these ICT systems increases rapidly. This increased dependency means that the implications of a cyberattack will have profound effects on the Dutch society.

We are on the brink of a boom of innovations that will take ICT systems even further into our society and increase the complexity of these systems. The Internet of Things (IoT) connects everything. Household appliances are nowadays equipped with WiFi, can be controlled through an app and communicate with their environment. Even more extensive: virtual robotics that are used in robotic process automation (RPA) followed by Artificial Intelligence (AI) where devices can make autonomous decisions, like self-driving cars.

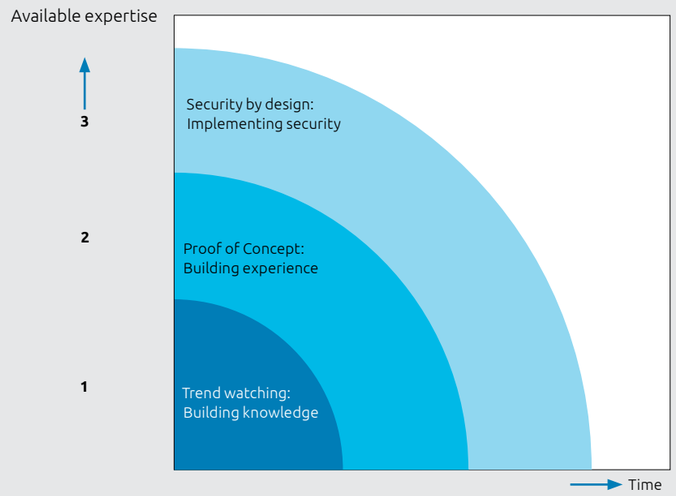
Our resilience

This increased dependency on ICT systems calls for well-functioning systems. Well-functioning systems reinforce our trust in these innovations. To secure this trust it is of great importance that our digital resilience keeps pace with the threats that impair the reliability of ICT systems. The crucial question that arises is: which possibilities does society have to withstand the gap between threat and resilience? Digitalization is unstoppable and innovations that are yet unknown to us (the 'unknown unknowns', introduced by Donald Henry Rumsfeld, former U.S. Secretary of Defense[2]) are already making waves. Luckily, we see developments where cybersecurity is included into product development. The European Union is proposing to help facilitate the quality of security products by means of certification[3]. Encouraging security in the design stage makes cybersecurity a focus point in the development of products and services and will consequently lead to goods that are inherently safe for use by civilians and organizations.

Coping with the gap

What is the best way to cope with cybersecurity and innovations like IoT, RPA and AI? Maturity of these innovations is obviously limited, and cybersecurity is usually not a focus point during development or introduction. It is of utmost importance that primary processes keep working properly and that no unnecessary risks are being brought on. What you could and should do is therefore dependent on how innovative technology turns out to be.

Figure 1: Innovation playbook.



When it comes to very innovative technology, like AI, it's wise to assemble expertise early on, not just about the applications that may benefit your organization but also about the risks that it might bring and how to contain those. See ring 1 in figure 1.

When it comes to technology that is new to your organization but has already been widely implemented elsewhere, like IoT, be sure to test the benefits and the risks through a Proof of Concept (PoC) and pay attention to cybersecurity precautions that your organization calls for. See ring 2 in figure 1.

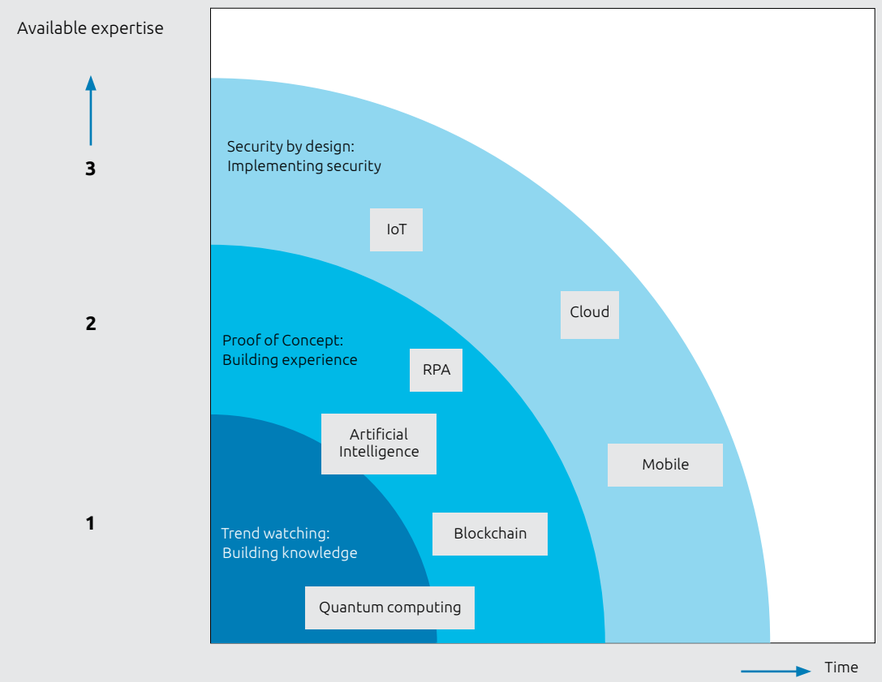
When applying new technology to your primary process make sure to identify all precautions and make them part of the implementation process through security & privacy by design. Also make use of phased implementation starting with non-critical business processes.

Every organization needs to fill in the innovation playbook according to their own ambitions. See figure 2 for an example.

The innovation playbook can be used as a tool to raise understanding at boardroom level when it comes to implementing innovations in a cybersecure manner. However, the innovation playbook can only be of real value when there is a general understanding of what cybersecurity means to the organization. If there is inadequate knowledge in the boardroom you need to bring up the level of understanding first[4].

So, has the gap been closed? Not yet. But you have made sure you have done everything imaginable to not stumble over innovation. Mind the gap!

Figure 2: Example innovation playbook.



About the authors:

Roger Wannee CISSP is principal consultant at Capgemini. He focuses on cybersecurity issues at public and private organizations.

Ton Slewe MBA CISSP is principal consultant at Capgemini. He focuses on cybersecurity issues at public and private organizations.

For more information you can contact the authors via:

roger.wannee@capgemini.com

ton.slewe@capgemini.com

[1] https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2017/1/CSAN2017.pdf. Note that the Cyber Security Assessment 2018 came to a similar conclusion (https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/cyber-security-assessment-netherlands/cyber-security-assessment-netherlands-2018/1/cyber_security_assessment_netherlands_2018.pdf)

[2] https://www.youtube.com/watch?v=GiPe1OiKQuk

[3] https://www.ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

[4] https://www.linkedin.com/pusle/brief-please-do-train-your-board-cyber-edward-amoroso/

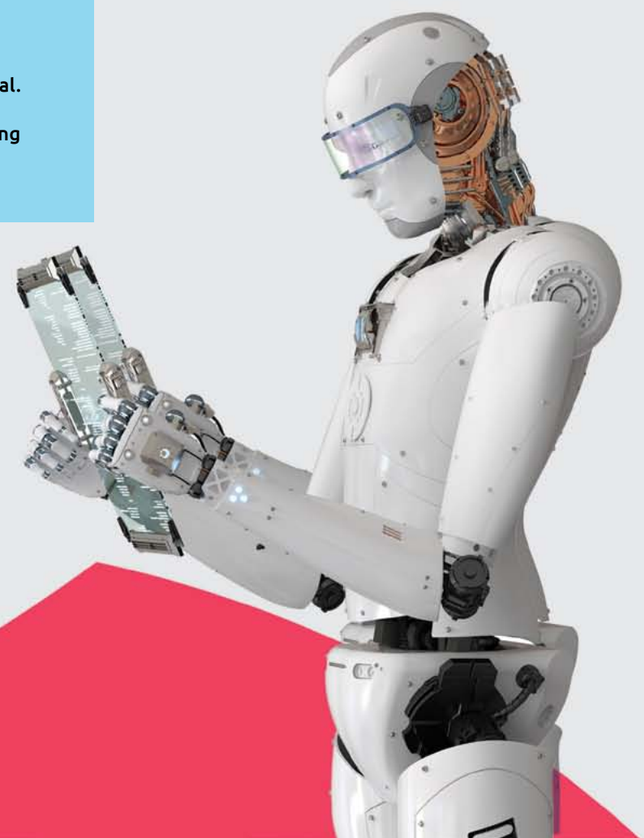
Trust me, I'm an algorithm

Are Artificial Intelligence systems reliable and if so, how do we prove this?

The arrival of Artificial Intelligence (AI) makes it possible for IT systems to make decisions that until now were solely reserved for human agents. Thus, making it of great importance that these IT systems are reliable at all times. Simultaneously, these systems are becoming more and more incomprehensible. So how do we prove their reliability?

Highlights

- **The arrival of AI enables technology to play an important part in the decision-making process.**
- **However, the way AI works is getting more complicated. Do we still trust this?**
- **AI systems can produce unintended and even unethical results.**
- **Choosing the right training data is crucial but not trivial.**
- **Complex AI systems generate better results but proving their reliability is difficult because of this complexity.**

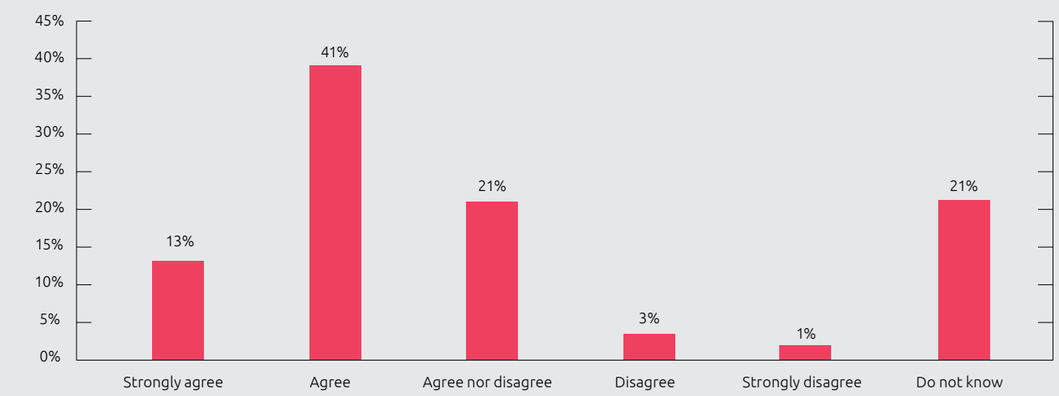


Gartner[1] and Forrester[2], among others, regard applied AI as one of the important strategical trends of 2018 and predict their march on to the system landscape in the years to come. This is also happening in the security domain: "predictive policing" uses dynamic predictions about where to expect crime to set in place police patrols and make the most out of scarce resources. Other systems are going through vast legal documents in the blink of an eye to extract relevant fragments and to predict or even make decisions.

With the arrival of AI we can identify two important developments:

1. Until now IT systems were being used to gather information. That information would then be interpreted by human agents and based on this interpretation decisions are made. However, AI systems are now evolving into being able to translate the gathered information onto a decision-making intelligence. Or they give advice on how to handle; for example sending out a patrol car to a specific street. On some occasions, IT systems already make decisions without human interference (self-driving cars, for example). Research from GfK, commissioned by Capgemini, shows at the same time that more than half of the Dutch population agrees that algorithms and AI are suitable for detecting digital crime on social media.
2. The algorithms used so far, to translate data into information, are invented by humans, coded by humans. That makes them comprehensible and relatively easy to explain. However, algorithms for AI systems usually come from a generic mathematical model containing a large number of (on their own meaningless) parameters whose values are derived from training the model on a great amount of historical data. This makes it almost impossible to explain how the AI system comes to a certain result. Reliability of the obtained results can usually be proven statistically but when it comes to proving an individual case it will become a "black box".

Algorithms and artificial intelligence are suitable for detecting digital crime on social media.



[1] https://www.gartner.com/newsroom/id/3812063
[2] https://go.forrester.com/blogs/top-technology-trends-2018-2020

Reliability of AI systems

Decisions made in the security domain can have profound effects. Think, for instance, of the Dutch media coverage when rapper Typhoon was pulled over in his car. Or the case of Bart van U., where the absence of involuntary committal led to the murder of former Dutch minister Els Borst. Officials in charge of making these kinds of (difficult) decisions have to meet high standards when it comes to impartial and ethical conduct. For civilians to be able to trust their government this impartiality and ethical conduct is key. And if IT systems are getting more and more involved in (assisting in) making these decisions without human interference then it's only logical that they should meet these high standards as well. For example: predictive policing relies on IT systems in deciding what kind of cars or which people should be pulled over in surveillance. We should be able to expect that variables like skin tone or religion should not be taken into consideration when making this decision. Making use of mathematical models and historical data sounds like a righteous approach in the matter. However, reality shows on multiple occasions that AI systems produce unintended results.

When the first virtual beauty pageant, led by an AI jury: "Beauty.AI", was held it resulted in mostly Caucasian winners. The system, on its own, issued lower scores to darker skin tones because the data which it was trained on did not entail sufficient representation of ethnical minorities. But even in cases where skin tone is not directly available to the system these kinds of results can occur.

In a segregated society, where zip codes are closely connected to ethnical background, we have to ask ourselves: is a zip code a valid indicator to help decide which car should be pulled over on surveillance?

Taking zip code into consideration may very well lead to a higher prediction rate with more justified pull overs and less unjustified pull overs. But it could also mean that people growing up on "the wrong side of the tracks" will be pulled over more often than others. This could mean that they could get in trouble for small offences easier than others. Which could in turn lead to difficulties obtaining a job. So, in the end, this model with a higher prediction rate could actually contribute to upholding segregation, or even enforce it. Using zip codes as an indicator in AI systems now has societal repercussions and needs to be considered very carefully. Whether or not certain indicators can justify certain decisions in a courtroom could give us a guideline on how to use them.

Another form of unintended and unwanted results is when there is too little reliable data available; the system will simply not have enough predictive power. In the United States of America teachers were evaluated by a system that compared SAT scores of their students at the start and the end of the academic year. However, difference in SAT scores is not solely dependent on teaching capabilities and the number of students per teacher was too small to derive solid conclusions. The same teacher can get great results one year, not so great results the next. Making decisions based on these kinds of calculations is basically nothing more than rolling the dice. AI systems are usually more complex but do stand at risk to these same threats.

Finally, there's the possibility of a system being used differently than originally intended. In Chicago an experiment started in 2013: Strategic Subject List. The goal was to be able to predict on a personal level which citizens were going to be involved in a shooting for the first time in the upcoming year and to minimize this by getting people the help they need. However, the approach sparked a great deal of debate because it focused on people who, at that time, had not yet committed a crime. This system also proved inoperable because of its weak predictive power. In the end the system was used to help find potential suspects to unidentified shootings.

Verifiability of AI systems

Even if an AI system is applied correctly and predicts or makes the (ethically) right decision it will only gain the trust it needs when the process and the accuracy of the result can be verified.

Verifying accuracy of the way an AI system works can be done in different ways, depending on de situation. In the most straightforward situation there is a "ground truth" that checks how often the system is right. If a system is designed to detect fraud, it's relatively easy to check if all the found results are actually cases of fraud and if all known fraud is being detected.

In most cases, however, a "ground truth" is not or very limited available. Systems that check for crime can not always be completely verifiable because some crime goes undetected. Some goes undetected because there are no charges filed, some because of the interventions that occur based on the predictions of the system. The results that were originally predicted never occur because of these interventions. But then it's still possible to verify the end result: does overall crime decline after applying the system? If it does it will always be debatable whether the decline is a result of applying the AI system or that there might be other forces at work as well.

It seems to be difficult, if not impossible, to prove accuracy of predictions of AI systems. It is however possible to fall back on another mechanism to gain trust: transparency. By disclosing the applied decision-making model everyone can assess the model and point out potential deficiencies. Transparency has, unfortunately, two major downsides. First of all, the comprehensible, less complex systems that are relatively easily explained, usually do not generate the same quality of results as more complex, less comprehensible systems do. They don't perform as well. Secondly, transparency is not always the way to go when it comes to decision-making models, especially when it comes to the security domain. Malicious minds could take advantage of this transparency and manipulate the system to stay undetected.

A last resource could be appointing an independent authority responsible for testing the accuracy of the systems without disclosing the way they work.

What's to gain?

Constructing an AI system that always comes to a (ethically) just decision is not a trivial matter. Proving that it is good and ethically just turns out to be difficult as well. But at the other hand: in the current situation, where human officials make decisions, the outcome isn't always a hundred percent either (see for example the well-known study "Extraneous factors in judicial decisions"[3]). So, demonstrating reliability of the decision-making process is, in fact, a step forward.

Furthermore is it certainly not unthinkable that in the years to come more and more AI systems will outperform humans (superhuman performance). When this happens a whole new business driver will come into being; it's not just about higher efficiency but about a true upgrade in quality and effectivity. But especially then, when AI systems seem to do certain things better then human agents do, trust in these systems becomes more important than ever! So, you better start early!

[13] **http://www.pnas.org/content/108/17/6889).**

About the author:

MSc Frank Inklaar is senior consultant at Capgemini. He focuses on applying advances analytics and Artificial Intelligence in the public and security domain.

For more information you can contact the author via:

frank.inklaar@capgemini.com

The Netherlands digitally secure: international collaboration as an example

When it comes to digital security; how can (international) collaboration be stimulated?

Highlights

- European collaboration of national CSIRTs is an example of how to strengthen our digital national security.
- Sharing operational security information is crucial to the security of our society.
- Enhancing trust and building towards converging ways of working will bring about increased collaboration.
- Trust Circles are a direct translation of trust relationships and collaborations on operational level within CSIRT communities.
- Cybersecurity could be more effective when private CSIRTs, organizational Security Operations Centers (SOCs) and national CSIRTs intensify collaboration.

Collaboration and alliances

Cyberthreats are becoming more imminent and come from all corners of the world. It's an illusion to think that an organization, on its own, can establish complete, effective cybersecurity. Inherently, there will always be a gap in information compared to the criminal. With the help of collaborations and alliances in sharing cyberinformation we can help make the word a more secure place. Establishing trust and clear agreements between our cybersecurity guardians is essential to effective collaboration.

Europe seeks further collaboration in cybersecurity

On September 13, 2017 EU president Junker said: "Cyberattacks can be more dangerous to the stability of democracies and economies than guns and tanks. Last year alone there were more than 4.000 ransomware attacks per day and 80% of European companies experienced at least one cybersecurity incident. Cyberattacks know no borders and no one is immune". The European Union has already taken legal precautions to improve the quality and level of cybersecurity within the EU. The European Parliament agreed to enforce the following European guideline in September 2017: "The Directive on security of network and information systems"(NIS). Member states had until May 9th, 2018 to convert this guideline into general, workable policy on behalf of cybersecurity. In the Netherlands, Minister Grapperhaus of Justice and Security sent the bill to the Dutch House of Representatives on February 15th, 2018. The NIS directive states that EU member states should have a national CSIRT (Computer Security Identification Response Team) equipped with sufficient organizational and operational tools. These CIRTS should collaborate to counteract cyberthreats. No distinction

is made between national threats or threats on EU level. Sharing of information without restrains (within the confinements of the law) is explicitly mentioned as a prerequisite to achieve international digital security. Legislation and a shared belief in the need for collaboration are pivotal starting points. This immediately raises the question of how to give meaning to this within the individual countries as well as inside the EU.

International collaboration makes the difference

National CSIRTs are, off course, already collaborating based on bilateral or multilateral agreements. Both within European borders (European Government CERTS-EGC) and worldwide (International Watch and Warning Network – IWWN) a lot of information, especially on operational level, is being shared already. This usually happens ad hoc and based on bilateral agreements that are initiated on an individual, personal level. An overarching policy-based framework, like the NIS Directive, is a recent development in order to develop further collaboration between all EU member states on all different levels.

Collaboration despite diversity and heterogeneity

There is great diversity in the origin of CSIRTS in different countries. Traditionally, and from their mandate, national CSIRTS are mainly focused on ensuring cybersecurity within national borders. This has resulted in a high degree of specialization on cyberthreats aiming for the vital sectors, vital processes and vital infrastructure of CSIRTs respective countries of residence. A side effect is a certain degree of compartmentalization of the information position of the various national CSIRTs. The origin of a national CSIRT also affects the operational behavior. It makes a big difference whether the CSIRT originated from academic context or intelligence context. This heterogeneity causes differences in maturity, openness and level of participation in the European network. Nevertheless, everyone agrees that international collaboration can make the difference in achieving success. Cyberthreats are by no means bound to borders. Having joint information at our disposal helps us operate more effectively. That's why information should be shared as effectively as possible. Sharing data is challenging when it concerns sensitive information and processing is subject to national legislation which differs per country.

Tools to build trust and share information

Increasing trust by means of trust circles

Within the (international) CSIRT community is one main determining factor for collaboration: trust. Trust in each other as individuals, trust in each other's organization, trust in each other's professionalism. Trust originates on an interhuman level through familiarity with one another.

"Trust circles" help us to gradually expand our network of trust. Trust circles are a direct translation of confidentialities and collaborations on operational level within CSIRT communities. Trust circles allow CSIRTs to specifically define with whom they are comfortable sharing information.

Every CSIRT has its own trust circle. This could be just one trusted partner, but it could also be a network of trusted partnerships. These trust circles can differ at any time and can also be dependent on current events, possibly even incident driven.

In addition, sharing information based on trust can also be strengthened by confining mandates and supporting tools. The NIS Directive is an example of a confining mandate on policy level. To a certain degree tools for information sharing are readily available. One example is TLP, Traffic Light Protocol, a classification standard that indicates limits on the redistribution of information. Trust in each other's professionalism is illustrated by mutually accepted standards to express intrinsic organizational maturity (SIM3, Trusted Introducer [TI] Certification Standard).

Converging ways of working help in sharing information

On operational level converging ways of working and compatible digital tools are essential. Such convergence simplifies the sharing of information and supports joint operations. When sharing information about incidents, threats or weaknesses it's crucial to come to an understanding about the meaning of the information, where it's coming from and how to handle it. A pivotal operational aspect is to come to an agreement about when to inform organizations and governments or when to stay utterly silent. It would be highly suboptimal if the investigation of CSIRT A gets frustrated because CSIRT B takes immediate, uncoordinated action. Successful execution of the NIS Directive framework is dependent on available practices and tools within Europe. In conclusion: trust and converging ways of working will result in increased collaboration. This is visualized in figure 1.

International collaboration as an example of digital security

The threat of cybercriminals is becoming more imminent and is coming from all corners of the world. The only way to fight it is to come together in collaboration and share weaknesses, threats and incidents. To achieve this we need increased trust between national CSIRTs and CSIRTs of individual organizations. A framework of trust has already been set in motion by cross-border regulation. The Directive on security of network and information systems [NIS]), CSIRT communities and direct human contact. In the Netherlands we already see much collaboration to increase cybersecurity. What is missing is sharing operational information between competitors and government. Trust circles can help with this in addition to aligning procedures on operational level. Converging ways of working and joint, generally available IT tools, but most of all shorter lines between organizations and independent cyber specialists, are to be desired. Governments need to enable the possibility of sharing information by resolving legal restrictions and increasing social acceptance.

Figure 1: Collaboration based on trusted information sharing, through converging ways of working, helps the CSIRT operation.

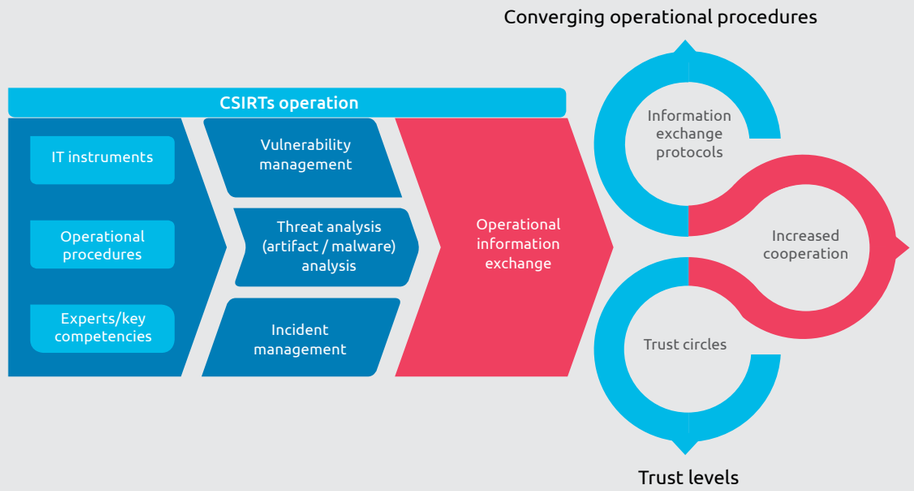


Figure 2: Is an organization allowed to gain competitive advantages by keeping information about cybersecurity as much as possible to themselves?

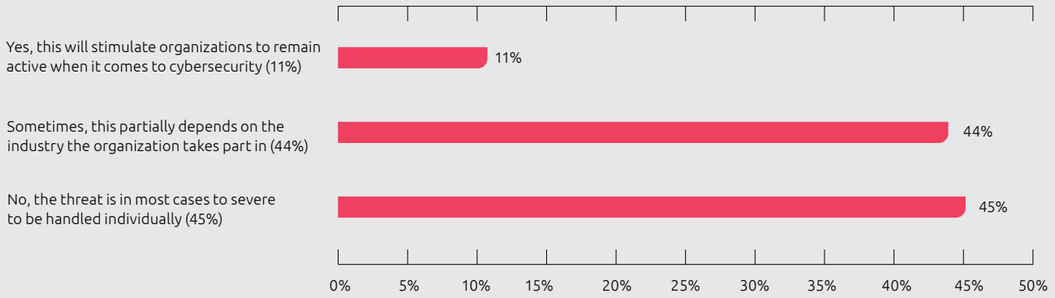
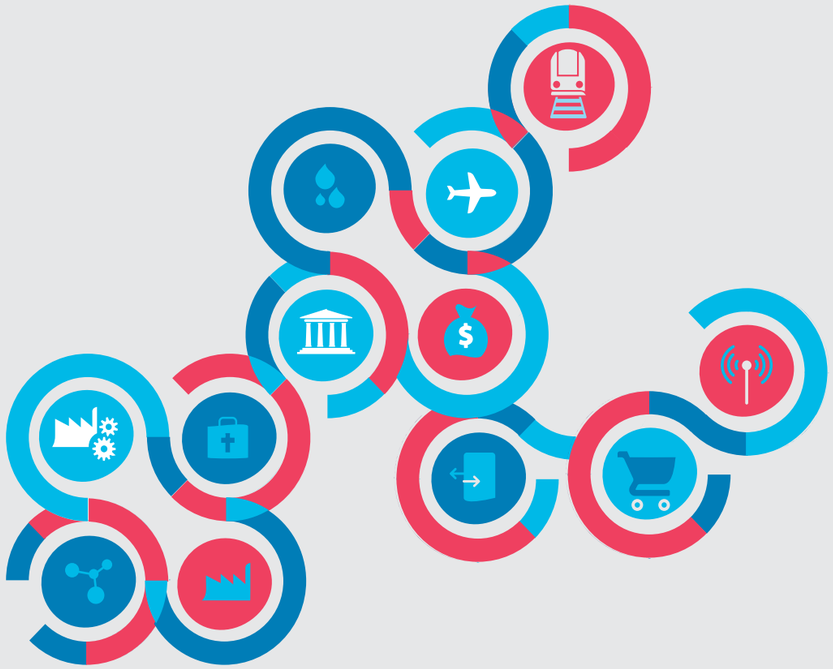


Figure 3: Circles connecting organizations.



About the authors:

Bart van Riel is managing consultant at Capgemini and enterprise architect. His focus is on balancing human and automated processes and optimizing business technology. He is also a mentor for aspiring architects within Capgemini and client organizations.

Jasper van Buren is a Capgemini consultant and specializes in the protection of confidential data. He gives tactical and strategical advice to organizations concerning (data) governance, policy and collaboration.

Roeland de Koning is a Capgemini consultant and specializes in cybersecurity and crisis management. He focuses on bringing about both national and international collaboration when it comes to these issues.

For more information you can contact the authors via:

bart.van.riel@capgemini.com

jasper.van.buren@capgemini.com

roeland.de.koning@capgemini.com

Improve security in the Netherlands by using data! But not at my expense

How can the public sector innovate using data & analytics without jeopardizing the security of civilians?

A more secure society by means of data & analytics or paramount privacy?

Highlights

- **Data & analytics can contribute tremendously to a more secure society.**
- **However, governmental use of data can provoke a feeling of insecurity in society.**
- **A DataLab offers great possibilities when it comes to tackle this conundrum.**
- **Because a DataLab expedites the search of solutions that increase security.**
- **And it also forms a foundation of trust in responsible use of data by the government.**

Using data to bring about a more secure society: a serious conundrum

The ongoing digitalization introduces various new challenges. One of these challenges poses a true conundrum: how do we use (for example personal) data to increase security in our society but simultaneously make sure that as a society we don't feel insecure because of this use of personal data?

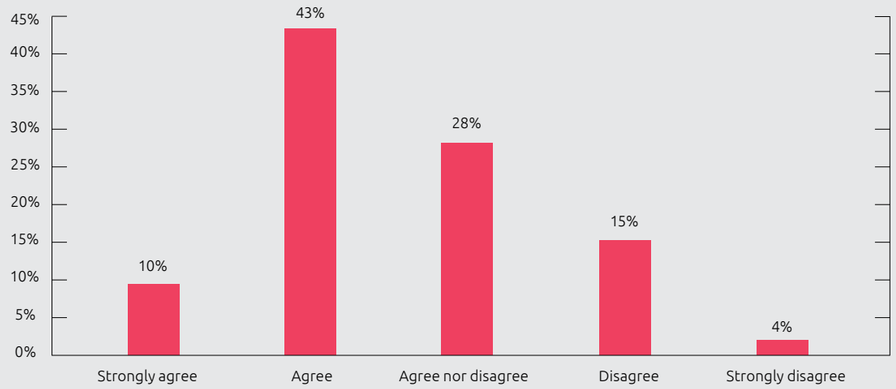
The process of gaining relevant insights by analyzing available data is called data & analytics. The data is usually available within a certain organization but can also come from outside the organization: from civilians, clients, partners, etc. Furthermore, data can be structured (in the form of tables or spreadsheets) or unstructured (in the form of documents and images). For analysis different techniques are used: statistics, econometry and Artificial Intelligence. In this article we focus on the opportunities data & analytics offer us in bringing about a more secure society. When it comes to security the following things come to mind:

- **Physical and social security:** that we will steer clear from experiencing physical harm (outside calamities). For example, criminal violence, accidents or meteorological events.
- **Financial security:** that our personal assets are protected but also protection of our communal tax revenue against fraud.
- **Digital security:** that our personal data is safe and cannot be misused for improper purposes.

Opportunities that data & analytics have to offer are, for example, better detection or even prevention of fraud and criminality. But while on the one hand experiments are starting in the public domain to investigate these opportunities we seem to encounter a reverse tendency on the other hand, regarding the use of data: there seems to be a rise in distrust when it comes to handling data. Is this data being used in a responsible way? Is my privacy ensured? Am I safe in this sense? Research by GfK, commissioned by Capgemini, shows that half of the respondents (53%) trust that the government protects their privacy sufficiently by legitimate use and proper storage of their collected data. 19% of the respondents questions this. Research conducted by Global Web Index[1] among Dutch internet users shows that 50% of them worry about the use of personal data by organizations.

[1] **GlobalWebIndex Market Report Netherlands Q2 2017**

Figure 1: . I am confident that the government uses my collected data legitimately, stores it properly and in doing so protects my privacy sufficiently.



The public sector takes promising steps

In previous years we have noticed a significantly increased interest in data & analytics within the public sector. This can partly be explained due to the growing demand for better performing governments and partly because those governments are in need of reducing costs. Here we can also identify two of the cornerstones of digitalization: the aim for higher effectiveness and higher efficiency. Organizations within the public sector are taking promising steps when it comes to data & analytics. A couple of examples:

Tax authority: strategic option for data & analytics

In 2015, the investment program of the Dutch Tax Authority was published. There was an unambiguous choice towards deploying data & analytics with aims of increasing tax revenue, more efficient procedures and satisfied employees. Fraud (detection and prevention) is also top priority.

Police: predicting crime

The National Police is also taking steps towards data & analytics and announced in 2017 that they would further extend the use of the Criminaliteits Anticipatie Systeem (CAS). This system predicts when and where crime, like a burglary, will be committed. In doing so the police is taking steps towards data-driven operations.

Data & analytics is still in its infancy state

These data & analytics initiatives within the authorities are encouraging but also need a critical remark. Just like in business, the learning curve of data & analytics consists out of trial and error.[2] We can make this out based on the "detached" way organizations bring on data scientist and start experiments. Mind you: there's nothing wrong with that! We need data scientists in order to achieve success in data & analytics and in the search of added value hypothesis-driven research (and also the validation of these hypotheses) is a main focus point. But the "detached" character of how things come to be indicates that we still are a long way from maturity.

Increasing distrust

The use of (even more) data also knows a downside. Besides generating value there is also the risk of damage. These risks originate for the most part from legislation. In the Netherlands we have various legislation that limits the use of data: the GDPR, the competition law and the Wiv (legislation on intelligence and security services). But there is also public opinion and as we already noticed: an increasing resistance against the use of personal data by the government and other organizations. When a few years ago ING Bank wanted to use personal data for commercial ends, huge protest erupted throughout society. The bank wanted to make use of client and transaction details

[2] **https://www.politie.nl/nieuws/2017/mei/15/05-cas.html**

to facilitate customized adds for other organizations. Even though everything was fine from a legal perspective the bank did not follow through on their plans in fear of impending reputational damage. Organizations who enthusiastically set out to use data & analytics are met with counterforce. They downgrade their ambitions in fear of slipping up. This would mean that the potential value of data & analytics, despite promising reviews, remains idle.

DataLab as successful approach to data & analytics

Experimenting is crucial when it comes to successful innovation through data & analytics. That's why we plead for a hypothesis-driven approach where promising innovative ideas are being led through an analytics funnel[3] (see figure 2).

Crucial part of this analytics funnel is the LabTest where the actual experiment takes place. The DataLab is the entity that executes the experiment. A DataLab entails, amongst others, the following components:

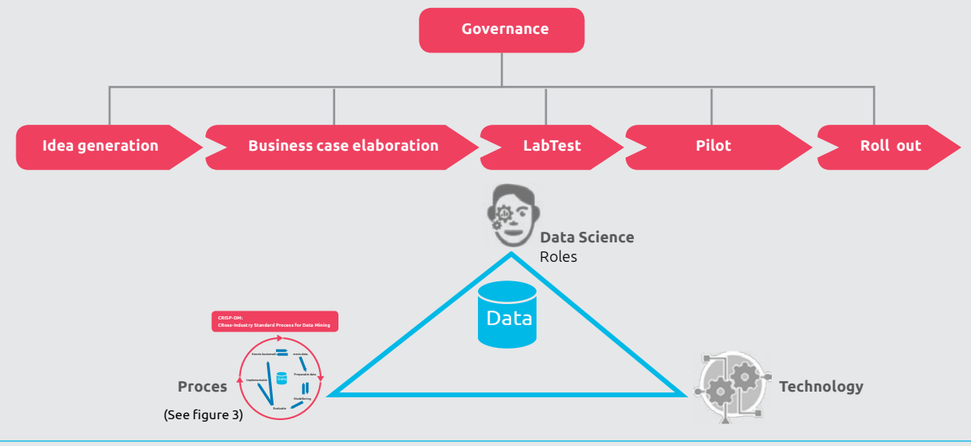
- **Roles:** the DataLab harbors various roles and the data scientist stands in the center of all of these. He (or she) is supported by other roles like a solution architect, data analyst and business analyst. It is of the utmost importance that experts of the field of operations are part of this team as well. Supporting roles like legal are also pivotal.
- **Process:** experiments in the DataLab are conducted conform the CRISP-DM-process[4] (see figure 3) that serves as a global standard for data & analytics projects. In this interactive process we gradually work from business issue to final implementation.
- **Technology:** the data scientist and other roles work on an analytical platform that facilitates a project-orientated approach and experimenting. In addition, this platform also ensures reusable analytical components and maps all steps from data to result.

A successful DataLab evolves by the continuous conduct of experiments. As a result skills and knowledge continue to mature. The DataLab, and the entire analytics funnel, deserves a place of its own in the organizational structure, including management and all. All of this should be embedded in a data & analytics strategy fueled by a hypothesis-driven approach.

DataLab supports trust

Trust in responsible use of data is an important condition for successful innovation through data & analytics. It is imperative for public organizations to demonstrate accountability at the use of personal data to achieve a more secure society. That is why this needs to be a vital part of the data & analytics strategy. And here's where the DataLab has the answer. The DataLab does not only help the data & analytics organization mature

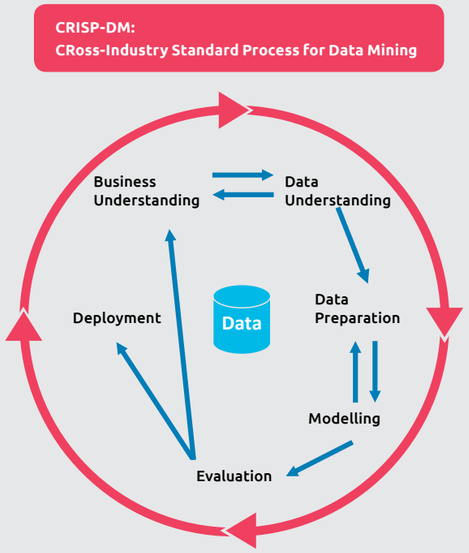
Figure 2: Analytics Funnel and DataLab.



[3] **Capgemini analytics funnel and DataLab model**

[4] **Shearer, C., The CRISP-DM model: the new blueprint for data mining, J Data Warehousing (2000); 5:13-22**

Figure 3: CRISP-DM model for data & analytics.



quicker but also ensures the proper use of data. Keyword in this is transparency. The DataLab approach ensures traceability of all steps, from innovation idea to implementation, through the use of clearly defined processes, control and technology. The following components are examples of this approach:

- **Traceability:** by making use of the analytics funnel, proper processes, and technology, all decisions can be traced. Even when certain steps are taken based on a model, it's always possible – by means of logging – to trace back the data and steps that have led to that result.
- **Model management:** when a model is being developed in the DataLab this will be actively managed when the operation kicks off. The model will then be updated in response to practical results.
- **Privacy Impact Assessment (PIA):** a PIA[5] is the aspect of the DataLab that ensures privacy. Needless to say, that this has be in accordance with the General Data Protection Regulation (GDPR)[6] that took effect May 25th, 2018.
- **Governance:** governance of the analytical funnel consists of evaluation that takes place at the end of every phase. We assess if the project is working towards the set goals by means of predetermined guidelines. It's possible to terminate the project after every phase if there is not enough validation of the hypothesis or if there are, for example, privacy concerns.

As part of the DataLab approach these components ensure continuous proper balance between the use of data and public versus individual interest. This way, all steps that are taken are not just internally traceable, but the organization can also inform their surroundings that they practice responsible use of data & analytics. It's a proactive way of diminishing public distrust.

Organizations in the public sector want to up their game by deploying data & analytics. However, movement in this direction is met by resistance. Skepticism and distrust from a society that also aches for better performances and increased security. To meet both demands (responsible security) we advise managers to set data & analytics as a strategic goal and embrace the corresponding professional approach. We are convinced that the DataLab plays a crucial part in this approach. Will, in a few years, data and analytics prove to be essential when it comes to making the Netherlands more secure? That partially depends on the tone of the debate in society. Managers now have the opportunity to positively influence that debate by making use of these components.

[5] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-impact-assessment-pia
[6] http:// autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/algemene-infomratie-avg

About the authors:

Daan Landkroon and Cyriel Houben both work at Capgemini. Daan specializes in implementing the DataLab approach. He also focuses on applying data & analytics to strategical issues in the public domain. Cyriel specializes in strategical issues cornering data & analytics and a DataLab.

For more information you can contact the authors via:

cyriel.houben@capgemini.com

daan.landkroon@capgemini.com

Who is taking action when our digital society is under threat?

How do we build trust in the digital society?

Highlights

- **Trust in the digital domain is important to further develop a free and prosperous digital global society.**
- **But digital attackers still have free game.**
- **Effective digital protection can't do without credible digital deterrence.**
- **A free digital society is implicitly vulnerable. The public needs to be aware of that.**
- **Current cyberwar incidents need to open for public debate.**

Our research shows that individual security perception is increasingly influenced by international security incidents. That's why cybersecurity is a recurring topic in various governmental policy papers, for example in the Foreign Affairs and Security strategy and the most recent Defense white paper. The question is whether this policy already resulted in a more secure digital society. In the physical domain security controls are usually clearly visible. But what do people notice of security controls in the digital domain? And even more important; do these controls actually discourage potential foreign attackers? What do we need to amplify these effects?

Security perception is a recurring topic in media and politics. It usually comes down to the discrepancy between actual measurable security and the individual perception of security for the public.

Less often it's about the international component of security perception. After being absent for many years, international security became an issue during the most recent parliamentary elections. And there was quite a lot to worry about: MH17, the Crimea, Trump, the Brexit, Erdogan, refugees, etc. This increased attention resulted already in a substantial reinforcement of the military budget facilitating further military equipment modernization and recruiting backlogs.

But do these reinforcements result in an actual increased level of trust for the people? And if not, what else do voters need to gain to have trust in our national security? Military capability is clearly visible during missions, extensive drills, open field days and ceremonial protocols. And this visibility contributes substantially to a sense of security. But these demonstrations of military capability are not only intended for national consumption. Equally important, or perhaps even more so, is the international radiance of military capability towards opponents and allies.

> *Hackers from the Dutch General Intelligence and Security Service (AIVD) provide crucial evidence of Russian interference in U.S. elections.*

Digital show of force

Military cyber capacity is now part of the capabilities of our armed forces. This raises the question: how could this capability contribute to civilian trust in the digital society? And how can this simultaneously deter our opponents: a "digital show of force", if you like. The 2018 GfK research, commissioned by Capgemini, showed that, just like the year before, people consider an attack in the cyber domain more likely than an attack in the physical domain. Research also shows that a major part of the population is not confident that the Netherlands are sufficiently prepared for a cyberwar.

If the people's sense of security is important – and debates prior to the 2017 parliamentary elections show it is – then it's up to politics and armed forces to show that our military cyber capabilities impress and are actually deployable. This trust is a prerequisite for further development of a free and prosperous global digital society.

How can trust in a digital society increase?

What is currently going on in the military cyber domain? Visible activities of the Dutch military cyber command are, among others, strategical contemplations in various national and international forums and small drills. But only cyber operations from the world powers really draw attention. Partially due to Snowden, we now know that the Americans have come a long way in this. This also showed from the Stuxnet operation in Iran. But there are, off course, plenty of other examples of cyber operations: Russia against the Ukraine, Georgia and the Baltic states. Capacities of China, Israel and Iran are also frequently subject of publication. The result of these events is that we now know that these nations have taken serious steps when towards the building of their cyber capability. What do we, the Netherlands, on our scale, have to match that?

Figure 1: Do you consider a digital attack on the Netherlands more likely than a physical attack?

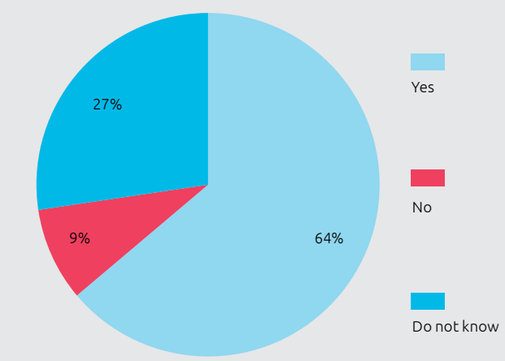
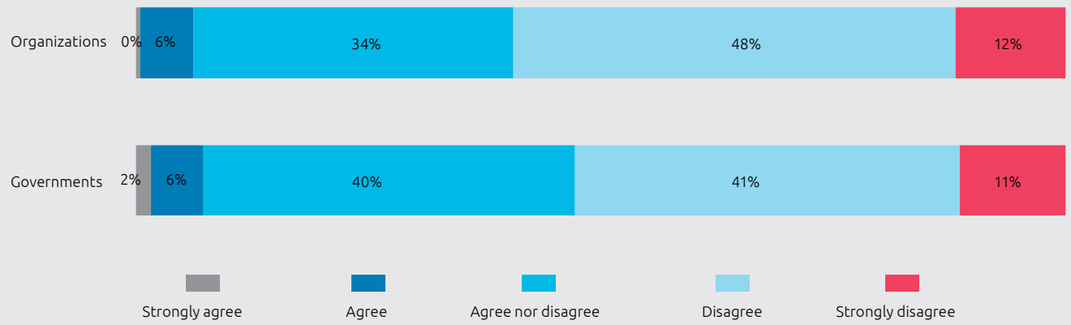


Figure 2: Dutch organizations/governments are sufficiently prepared for a possible cyberwar.



Publications in the Dutch quality newspaper de Volkskrant about the cyber capacity of our intelligence services concerning Russian interference during the U.S. elections have left quite an impression, both nationally and internationally. A sensational narrative about the way of conduct shows that, apparently, we not only have an advanced cyber capacity at our disposal but also have the insights to put it to use and maximize its results. But that's not the only thing that's special about this incident. While a similar military operation in the physical domain would immediately and noisily be countered, now seemingly little happened. So the threshold for conducting operations in the digital domain appears to be lower. It also seems that this cyberwar has been going on for a while now, but that it's mainly an issue of and between intelligence services and is kept away from the public eye. On the one hand one might propose that this a good thing because it will not deepen the perception of insecurity amongst civilians.

On the other hand with this cyberwar out of the public eye there is no real sense of urgency with organizations or civilians to take precautions in order to increase (their) security. Armed forces and intelligence services will not directly suffer from this but society as a whole just might. Because to civilians it remains unclear whether the periodical disruptions in public services are 'regular' disruptions or that they are the result of cyber hacking security services.

Protection of the globally free digital society

No matter how thick your digital protection wall may be, there will always be some weak spots and there will also always be attackers defying them. Undermining our western law and order and alliances is a recognized objective from our opponents.

> *The defensive form of war is not a simple shield, but a shield made up of well-directed blows.*
>
> **Generaal Von Clausewitz**

That's why security has a moral side as well: the willingness to take the punches and make some sacrifices because we are convinced that our goal, a free, digital international society, is a universal human right. And that a digital society limited to a particular country or region doesn't comply to this concept only, but will actually lead to further weakening of the public resilience. This moral resilience, these collective coping capabilities, are currently under pressure. Think for instance about the Ukraine referendum, refugee debate or the Brexit.

Resilience

Analysis of cyber incidents often show that a specific attack wasn't particularly sophisticated in itself, but the victims failed a proper basic protection. Resilience is defined as the combination of knowledge and awareness amongst civilians, technological security measures and the capability to get back on your feet quickly after a crisis. Strengthening our digital resilience is our common responsibility. But enhancing this maturity when it comes to living up to our responsibilities requires even more attention and investments. This is out-of-scope for our armed forces. They only might be called upon to support civil authorities in the case of (a digital) disaster.

Digital combat capabilities and digital human rights

According to international law experts a cyberattack might be retaliated in the physical domain. From a strategic point of view this is however not very realistic due to the unpredictability of the effect and the risk of further escalation. Attribution remains complicated as well: are you sufficiently sure of who is behind the attack? And finally retaliation must be proportional and subsidiary. And so, if physical retaliation is not opportune you are left to react with cyber.

This retribution capability should be well known to the broad public. Some might say that this form of deterrence results in honeypot effects, attract (even) more attacks and thus contribute to a spiral of cybercrime. It can also attribute to the expansion of military cyber industries and further proliferation of cyber weapons to undemocratic regimes. This could all be true. Just as true as it is, and was, within the analogue domain. But the alternative, digital pacifism, is definitely not a solution either.

As stated before, resilience is not just providing digital security measures. Contributing to international law and order, which also entails the digital one, is another key task of armed forces and of great importance when it comes to our values of democracy, human rights and the constitutional state. Our military digital capacity has to be suited to contribute to this as well. It's important that these capabilities are visible to the public but also to the dissidents far away and especially to their oppressor.

Conclusion

We have to protect ourselves digitally, this goes without saying. We do however need a capable and visible apparatus to help us along. An apparatus that, if need be, is able to strike back fiercely. The attacker needs to know up front that this retaliation will actually happen and that it will hurt, a lot.

In the end it has to become possible to deploy our military capability in order to ensure digital international law and order and human rights. This can lead to consequences when interventions bring along repercussions. The potential sacrifices we have to make are definitely well worth it. Not only because our inventions contribute to a better world but also because of the credibility of our values and the essential public support for the digital armed forces.

About the author:

Peter Kwant (Executive Master Security & Defense) is principal consultant cybersecurity at Capgemini and former navy officer.

For more information you can contact the author via:

peter.kwant@capgemini.com

Is Big Brother the new future?

Do potential security and terrorist attacks require more openness and collaboration between people, companies and governments?

Highlights

- **The GDPR[1] and Wiv[2] laws demand more collaboration between companies and governments.**
- **Protecting the safety and privacy of civilians inevitably creates more transparency between people, companies and governments.**
- **Developments in technology facilitate more openness and collaboration between civilians and governments.**
- **Technological developments will bring about a change in people's behavior, both in their professional and private lives.**
- **Rapid developments in technology demand rapid, standardized Agile developments of Security IT solutions, especially automated security software.**
- **Non-functional IT solutions will become more important.**

The fragile balance between security and privacy

Public opinion about intelligence services changes quickly. "When Eric Snowden is on the news, everyone worries that secret services gather too much information. But when a terrorist attack happens in Europe people are worried that we don't do enough in the Netherlands to prevent this from happening here as well". This is wat Minister Plasterk said in his speech at the University of Amsterdam during the Dutch Presidency of the council of the European Union. "Finding the right balance between security and privacy is extremely difficult to achieve", he says. "You could argue that there is no conflict between them. Privacy is a human right. But security is a prerequisite to be able to enjoy that human right". That's why it is imperative to find a right balance between privacy and security.

As of the 25th of May, 2018 European Union privacy is legally represented by the law Algemene Verordering Gegevensbescherming (also known as AVG or GDPR[3]). The primary goal of this legislation is to protect personal data. Security is protected by the Wet op de inlichtingen- en veiligheidsdiensten (Wiv) or the so-called "dragnet" law. It allows the intelligence and security services, AIVD[4] and MIVD[5], the ability to investigate data to see if it signals potential terrorist or cyberterrorist attacks. This law also ensures the right to privacy.

Both pieces of legislation, the GDPR as well as the Wiv, must use security IT solutions. These solutions, however, go hand in hand with several challenges. The main goal of this article is to find out how we can protect our civilians but also how we can ensure their privacy in the years to come. A few questions are pivotal in doing so:

1. How can EU countries ensure the privacy and security of all EU citizens and EU countries in the next 5 years?
2. How are both people and technology going to develop in the next 5 years?
3. What kind of impact will legislation like GDPR and Wiv have on the way people and technology change and how do we adjust security IT solutions to these changes?

New GDPR legislation, what does it mean for EU citizens

The GDPR defines important guidelines to ensure the privacy of personal data[6]. The primary focus is processing personal data in a legitimate, honest and transparent way in relation to the persons the data concerns. In addition, there needs to be adequate security of personal data. Data may only be stored and used when circumstances call for it ("need to know") and may only be accessible to personnel that use the data for business purposes. Personal data may furthermore only be used for clearly stated, legitimate purposes and may not be stored any longer than is necessary. Access to personal data can only be possible after consent from the person or persons in question.

Wiv: legislation regarding intelligence and security services

The current legislation, dating from 2002 is limited in its effect. If the AIVD sticks to traditional intelligence practices like shadowing, observing, intercepting phone calls, wiretapping and so on they will miss crucial information. The new 2017 legislation provides the AIVD with contemporary capabilities to investigate data to see if it contains threats and ensures the right to privacy. This goes hand in hand with better inspections that occur before, during and afterwards. Data may only be collected and stored when it relates to investigations that were commissioned by the government. All other data may not be collected or stored by the AIVD.

Terrorists, extremists and spies use chat applications and communication channels like WhatsApp, Telegram and Signal. These applications exchange encrypted information. The U.S. government already tried to find a way to obtain access to this encrypted information but did not succeed[7]. Therefore, Wiv legislation does not focus on encrypted in formation but on metadata instead[8].

GDPR and Wiv: Security IT solutions

In real life this means that security IT solutions must be able to support the demand for information at one hand but on the other hand also have to be able to ensure privacy. This means that Wiv will set standards for the collection of (meta)data.

[1] General Data Protection Regulation is European law on EU citizens data privacy, https://eugdpr.org/.
[2] "Wet op de Inlichtingen- en Veiligheidsdiensten", Dutch law to support intelligence and security services in stopping terrorist and cyberterrorist attacks.
[3] General Data Protection Regulation is European law on EU citizens data privacy, https://eugdpr.org/
[4] Algemene Inlichtingen- en Veiligheidsdienst conducts research in Holland and abroad to identify national security threats and risks, www.aivd.nl.
[5] Militaire Inlichtingen- en Veiligheidsdienst delivers intelligence information to the Dutch armed forces, http://www.defensie.nl/mivd/.
[6] PII is personally identifiable information that can be used on its own or with other information to uniquely identify an individual.
[7] https://en.wikipedia.org/wiki/Skipjack_(cipher)
[8] Data about the communication, for example, the telephone numbers, location, start and end time of a conversation.

GDPR will also set standards when it comes to protecting access to personal data and will focus on evidence of this protection.

For the Wiv a general security IT solution is expected with AIVD and MIVD employees as end users. Every organization needs its own GDPR security IT solution that needs to be approved by an external certification process. Organizations that fail this inspection and fall prey to security breaches can be fined up to 20 million euro or 4% of their total revenue. It is the end responsibility of governments in the EU to balance national security against privacy for their citizens. Companies in the EU need to balance their business privacy against privacy for their customers.

All security IT solutions for GDPR have the same objective; ensuring privacy for the individual. The Wiv has a different objective. However, both IT solutions need to be able to function as one on the internet. Technology is improving and changing rapidly; more applications, new types of devices and solutions are being connected to the internet. Consequently, the internet and the number of people using it is still growing. It is of paramount importance that the IT security solutions used to support GDPR and Wiv keep up with changing technology. What are these technological developments that we face in the near future? And, more interestingly, how can we deal with them?

Technological developments

It is almost impossible to keep up with new technological developments. In this day and age, it is essential to try and predict the future, something that few people contemplated 50 years ago. We live in a dynamic and innovative period and experience many technological developments. Some examples of technological trends within the next 5 years[9] are:

- Faster and more complex possibilities to analyze connections between (even more) Big Data
- Controlling and monitoring through IoT
- More robots and less jobs (automation)
- Real-time health recognition (e.g. FitBit)

These trends will bring about changes in our surrounding, something that we will have to adjust to. Darwin's theory of evolution may be 150 years old but is still very relevant these days. His theory of evolution explains how vegetation, animals and humans have evolved from their ancestors and adjusted to their surroundings by means of natural selection[10]. Changes in technology also brings about changes in our surroundings and we must adjust our behavior accordingly . Change in our behavior can occur faster than change in our genes. Human beings, contrary to other animals, can choose proactively when it comes to their behavior in certain surroundings.

The opportune question is how do we deal with this as a society? These technological developments could be used to improve the intelligence services of our government and help strengthen national security. But there's also a downside when it comes to these technological developments: how do we ensure privacy and how much access do we allow our government?

More transparency and standardized security IT solutions

How can EU countries ensure the privacy and security of all EU citizens and EU countries in the next 5 years?

Regulation compels EU countries to protect personal data on the internet. Showing evidence that this data has indeed been protected is becoming more important. Security IT solutions will not only be a key factor in the protection of personal data but they will also be of great importance in detecting terrorist and cyberterrorist attacks. These solutions can predict potential attacks by using personal and metadata. This could in turn give the intelligence and security services a considerable advantage in staying one step ahead of terrorists and cyberterrorists. A major issue with the Wiv law remains consent and access to data, especially decoded (or non-encoded) personal data.

All security IT solutions for GDPR and Wiv need to function invisibly on the internet. They need to be flexible, quick and easily adaptable because new risks and potential threats can appear quickly and existing ones can change rapidly. Following on, standardized solutions (general IT and Security IT) are inevitable because this is the only way to meet all solution requirements: efficiency, speed and high quality. A main aspect of design and development of all security IT solutions (and general IT solutions) are the non-functional requirements[11]. Examples of these non-functional requirements are: reliability, usability, compatibility, maintainability, portability and performance[12].

[9] http://research.ibm.com/5-in-5/

[10] https://nl.wikipedia.org/wiki/Evolutietheorie#Principe_van_evolutie

[11] Quality attributes, http://iso25000.com/index.php/en/iso-25000-standards/iso-25010.

[12] Optimal use of computing resources to provide fast results from the processing of data.

How are both people and technology going to develop the next 5 years?

Technology will take over more tasks from people, especially when it comes to the working environment. Technologies will become more intricate but also more user-friendly. It is important to raise awareness on the devices that are being connected to the internet (think of IoT) because many of these devices are by default not secure and they can be used for communication in unpredictable ways. It is important that the suppliers of these devices develop their products with security in mind and make it easy for customers to protect their devices. Examples are: improving general knowledge of managing passwords; secure programming; managing OS Patches[13] and; secure control and monitoring with IoT devices.

What kind of impact will the GDPR and Wiv legislation have on the way people and technology change and how do we adjust security IT solutions to these changes?

Security IT solutions need to be easily adaptable to changes in security threats and vulnerabilities. This is similar to the continuous development and implementation of software through an Agile approach. A major component is advanced automated security software to support existing and aging IT solutions.

In summary: technology is developing rapidly. Consequently, the IT landscape is subject to rapid change. When it comes to transparency between civilians and their government there needs to be a shift in mindset. This does not mean that there needs to be full transparency of personal or business-related data. It does mean that there needs to be transparency of what, where and when data is being processed. This is the only way to learn from mistakes and to improve security IT solutions, but it is, ironically, also the only way to protect people and their data. Not Big Brother[14] is the future!

[13] Installation of solutions to security weaknesses in operating systems. Examples of operating systems are Windows and Unix.

[14] We hope to see an open society and government in the future not a society run by dictators as George Orwell warned us in his book 1984, https://en.wikipedia.org/wiki/Big_Brother_(Nineteen_Eighty-Four).

About the authors:

Kim van der Veen is employed by Capgemini Invent and focuses on the importance of raising awareness of human agents and cybersecurity.

Barry Jones is employed by Capgemini Invent. He specializes in software development, general testing and security with a focus on IT governance development of these subjects.

For more information you can contact the authors via:

kim.vander.veen@capgemini.com

barry.jones@capgemini.com

Fake news and disinformation in the security domain

How do we prevent fake news from impacting our security?

Highlights

- **Due to technological developments the reliability of information is under pressure, now more than ever.**
- **This trend can bring about far-reaching and imminent consequences within the security domain.**
- **Tackling this problem requires a joint approach from both civilians, organizations and government.**
- **Extreme caution is recommended when it comes to regulatory measures.**
- **Security services need to make a strong play on technological tools - The government needs to support civilians by raising awareness about this subject.**

Reliability of information is under pressure, now more than ever

"A lie can travel halfway around the world while the truth is putting on its shoes". Mark Twain's saying is more relevant than ever; how (un)reliable is information this day and age? Fake news, currently much debated, is also a form of disinformation. No self-respecting news channel can function without fact checkers. Distribution of incorrect information in political campaigning especially, is a hot topic in current debates. We are being cautioned, both nationally and internationally, against consequences and dangers that come along with the spread of targeted disinformation. But do not be mistaken: manipulation through targeted (mis)information is as old as politics itself. Propaganda techniques, which aim to disrupt and destabilize the opponent, have been incorporated in political campaigns for ages. The problem in our day and age is that by virtue of current technological developments this can be done ever so subtly and with incredible reach. Assessing reliable information on our own becomes harder and harder. We could be on the brink of not being able to tell real video fragments from digitally simulated ones, except by making use of technology. In our current, dense society, where information is widely spread through digital platforms, it has never been easier to reach so many people and cause disruption by merely broadcasting a message. These developments make it extremely difficult to separate reliable information from unreliable information in proper time. And this effects the entire society.

Disinformation imposes direct dangers

In the security domain the danger of disinformation is also very relevant. Reliable and timely information is of crucial concern, especially when it comes to crisis management and preventing security incidents. First coverage of events usually comes from social media, traditional media seems to follow after. This is problematic because it takes (a lot of) time to verify if what is being said is actually true. And currently we do not have that time; everything needs to be on demand! This desire to have all information instantly available erodes the validity and reliability of information. If the truth ever gets done putting on its shoes and catching up we have to wonder: is it too little, too late? Targeted disinformation can have a direct effect on our security. The following fictitious scenario illustrates this:

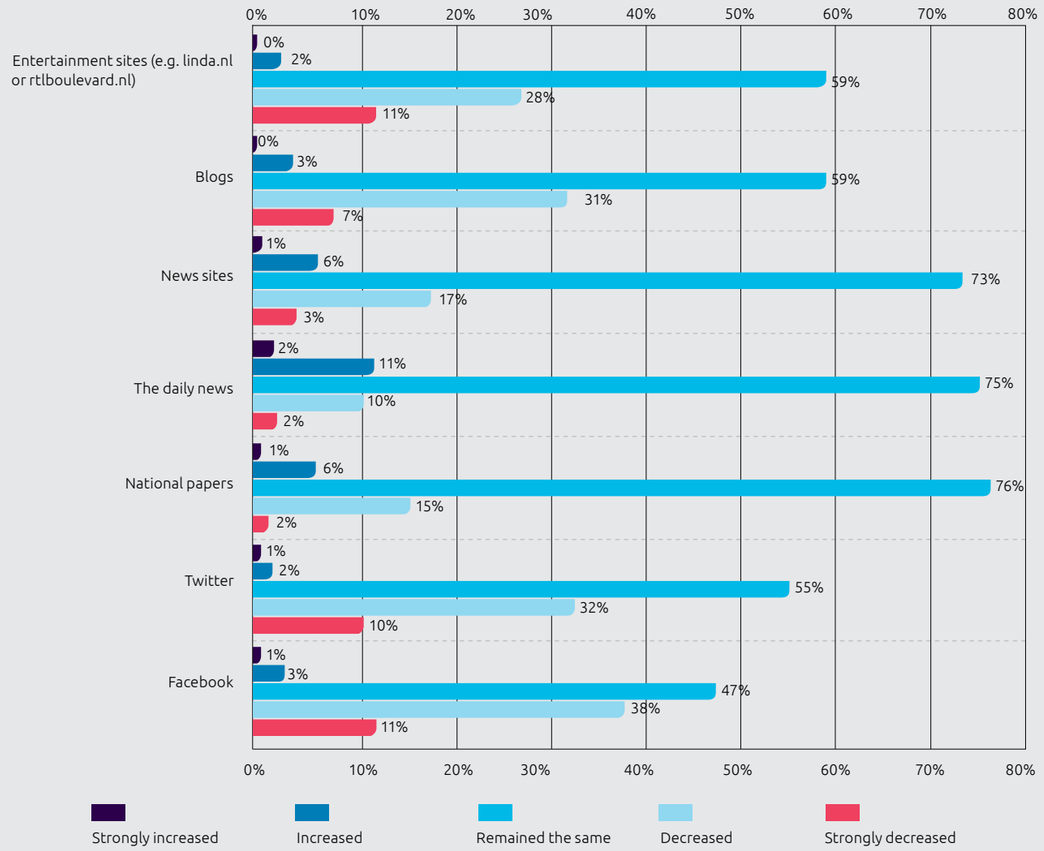
Fictitious scenario

There has been an explosion at Utrecht Central train station. Both cause and number of victims are unknown. Within minutes the event is trending on Twitter and getting a lot of attention on other social media as well. Soon, reports are saying it is an attack. Online platforms are reporting contradicting numbers of victims, varying from fifty or so to several hundreds. There are no official statements as of yet. A little later, on a digital platform, the alleged attacker is identified, and a public manhunt starts to find this person. At the same time rumors are spreading on social media: terrorists have indicated that there will be another explosion at another train station. Within an hour of the event massive panic sets in and it becomes a national matter closely monitored by security services.

When the dust has settled all this turned out to be a very refined disinformation campaign set in motion by a terrorist group. Paid distributors (so-called trolls) were hired to spread incorrect information about the number of victims in order to create chaos. Reports about a second attack were spread by making use of automated social media accounts or "bots". The identification of the alleged attacker was plain wrong. It was the unintended result of a crowdsourced investigation; an online search by digital volunteers on online platforms.

This scenario shows that both unintended and deliberate disinformation can bring about security risks. Trolls and bots can also be used my malicious minds for other purposes than political manipulation. In Sweden, bots were used to create social instability by spreading false stories like a Muslim man destroying a church.[1] In the Netherlands there was a 27-year-old man posing to be a relative of one of the MH-17 victims. He deliberately distributed disinformation to disrupt the ongoing discussion about the crash.[2] But even unintended disinformation can lead to catastrophic results. The manhunt from our fictitious scenario may seem farfetched but during the Boston Marathon bombing in 2013 a young man was wrongfully identified as the alleged perpetrator on social media platform Reddit. The young man had been missing at the time and, as turned out, had nothing to do with the incident. This incorrect information was picked up by a lot of other platforms, including news channels, and let to an unjustified manhunt and unpleasant results. The family of the alleged perpetrator was harassed through phone calls, emails and Facebook messages about their supposedly terrorist son. About a week later the drama came to a conclusion: the young man was found dead. He had committed suicide even before the bombing happened. This shows that both deliberate and unintended disinformation can bring about far-reaching consequences in our current, digital era.

Figure 1: To what extend has your trust with regard to following media increased or decreased?



[1]BBC News 04-01-2018) 'Swedish security chief warning on fake news', abstracted from http://www.bbc.com/news/world-europe-42285332.

[2]RTV Utrecht, (15-01-2018) Nieuwegeiner geeft nepnieuws over MH17 toe. Https://www.rtvutrecht.nl/nieuws/1717124/nieuwegeiner-geeft-nepnieuws-over-mh17-toe.html.

It is time to take precautions

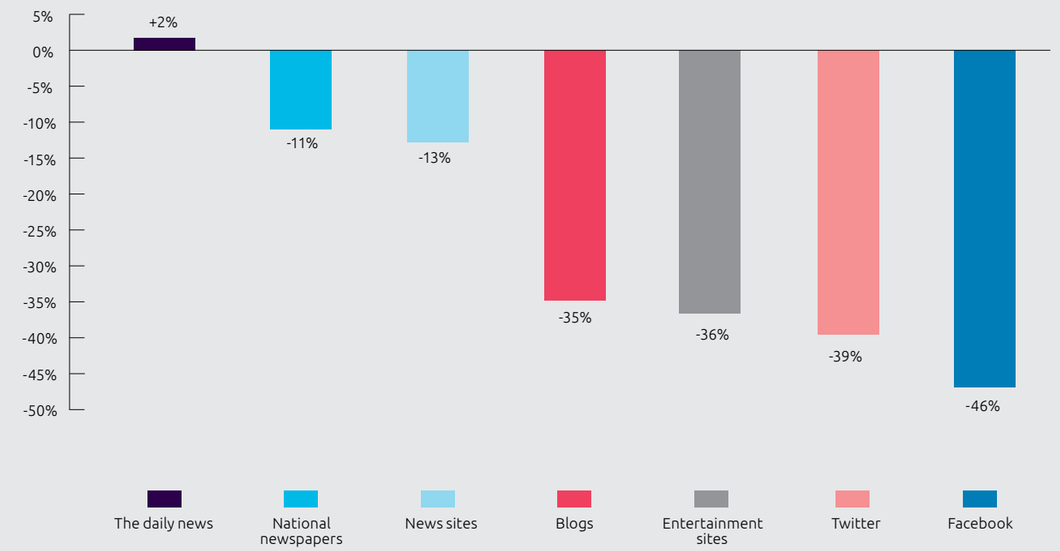
Civilians are losing faith in the accuracy of reporting, partially because of the growing part social media plays in this reporting. Trust in the reliability of almost all forms of media has again decreased this year shows research from GfK, commissioned by Capgemini. Only the daily news shows a small increase in trust. Trust in information on social media (Facebook, Twitter, blogs) has decreased tremendously compared to trust in traditional media like the daily news or newspapers. Generally speaking, trust in the media has decreased less with people with a low educational level and young people (18-29 years old) than with people with a higher educational level and elderly (50+).

We are mostly focused on the impact of (un)reliable information in politics but we must also steer our attention to what the impact could be in the security domain. Disinformation can have far-reaching impact when it comes to security incidents. To prevent this development from having major impact on our security we need to take precautions. Like all the threats we are trying to withstand these days it is crucial to bring together everyone who is involved and take action together. Tackling disinformation is a joint responsibility.

Fine line between regulation and censorship

To get a grip on the problem of disinformation multiple governments have looked into regulation. They hope to contain disinformation by drafting strict regulations and establishing watchdog organizations. In Indonesia an agency was founded to monitor online news and counteract fake news. Closer to home, Germany has implemented legislation (the Netzwerkdurchzetsungsgesetz) that makes it possible to fine digital platforms up to €50.000.000 to enforce them to remove hate speeches and disinformation within 24 hours from their platforms. This lead to heated debate because this comes dangerously close to censorship. It's exactly why the recently founded agency EU vs Desinfo, a similar watchdog of the EU, also made headlines. Sharp criticism arose from the Netherlands when this agency blacklisted several platforms and marked them as distributors of disinformation. From all corners of society, including prominent late-night show "Zondag met Lubach", well respected Dutch newspaper NCR and entertainment website GeenStijl, protest formed; this was containment of freedom of speech and thus unacceptable. This shows that it's of the utmost importance to apply extreme caution when it comes to regulation.

Figure 2: Precentral increase and decrease of trust regarding media.



Invest in technological capabilities

The government plays an important role when it comes to validating information concerning a security incident. An investment in technological capabilities conducting online forensic research is needed in order to evaluate the reliability of online information. Technology makes it possible for “bots” to distribute disinformation but there are also innovations that help detect incorrect information. There have been multiple experiments with digital tools (like blockchain experiments) to filter and counter fake news. Explicit online presence is a must: it is the only way to contain the consequences of unvalidated online information. Swedish security services have made this one of their top priorities. They make a great effort to inform civilians through, for example, Twitter. Instead of just informing people about validated information it’s equally important to speak out about information that has not (yet) been validated.

Technological organizations and online platforms have to take responsibility

It is crucial to stimulate (online) platforms to take responsibility for the information they distribute. Never before was it so important for the news industry to uphold journalistic standards. Even social media platforms can invest in technological tools that are needed to detect disinformation. Recently Facebook announced the implementation of “bots” and Artificial Intelligence in order to counter fake news. We can also try to find ways to “rate” and classify online information. Wikipedia has been using a system where information is verified by volunteers. Facts are being checked and articles can get a “tag” if accuracy is challenged.

Digital literacy

Civilians, off course, have a responsibility of their own as well. Every individual has, in a certain way, the possibility to conduct journalism by collecting and distributing information. This brings along a certain responsibility. The origin of information and the reliability of sources must be the focus of attention. Algorithms in social media make sure that people mostly see what they are interested in. This eventually leads to filter bubbles and echo chambers. Following multiple sources of information is crucial in order to avoid a unilateral view. To lure users to their website online platforms, make use of tantalizing headlines. It is up to civilians to be skeptical of sources of information. In order to do so you need a certain level of online maturity, of digital literacy. It is up to the government to support civilians in developing certain awareness and behavior when it comes to dealing with online information. This can be achieved by initiating and financing programs that stimulate digital literacy. Educational institutions hold a key position when it comes to improving digital literacy, both for the young and for the elderly. In the U.K. for example, a collaboration has started between the National Security Council and the BBC to educate youngsters on this subject.

Will the truth prevail?

Several sides have to make a move to prevent fake news from impacting our security. Close collaboration between government, technological organizations and civilians is crucial in working towards reliable reporting. The government needs to be extremely cautious when it comes to the quandary of regulation vs censorship. The government also needs to invest in technological capabilities to make detection of incorrect information possible. This is a joint responsibility shared between government, technological companies and online platforms. And most important of all: the civilian. It is impossible to completely prevent incorrect information. That is why, to deal with this incorrect information, we need to greatly improve the online maturity of our society.

About the authors:

Bart Bikkers, Fokko Dijksterhuis and Martien Hols are all operative at Capgemini Invent. Bart focuses on issues concerning privacy, national security and crisis management. Fokko focuses on the organizational and human aspects of cybersecurity. Martien focuses on matters in the security domain, mostly from a financial perspective.

For more information you can contact the authors via:

bart.bikkers@capgemini.com

fokko.dijksterhuis@capgemini.com

martien.hols@capgemini.com

Ambassadors gain trust between security and business

How can ambassadors gain a better collaboration between security and business?

Establishing and deploying ambassadors within an organization ties together various fields in the organization like security and daily operations.

Highlights

- **One of the most challenging things for a security department is to have a strong connection to all business units of the organization.**
- **Insufficient connectivity to business units increases the change of security breaches like releasing insecure products or services.**
- **Ambassadors bring cohesion between the security department and the entire organization.**
- **Inspire and train a network of ambassadors to fully incorporate security into the culture, DNA and all operations of the organization.**

It's not uncommon: project leaders asking the security department to quickly check if the service they want to deploy next week is actually secure. It's a textbook example of why there is an urgent need to bridge the gap between the security department and all other business units in the organization. In this article we will outline how we can achieve this.

Many organizations, inside and outside the security domain, are in the process of taking precautions to improve their resilience when it comes to security. This process is being sparked by both physical and digital risks and threats. Too often speed is of greater importance than security which in turn leads to the release of insecure products or services. Security is usually seen as slowing down the process of development and something that brings about a lot of work. As a result, this leads to a gap between business (daily operations within the business units, departments or divisions) and security. A result that is highly unwanted because profound collaboration between business and security lies at the heart of a secure organization.

Bridging the gap by connecting

Organizations use new practices and take new measures to bridge the gap between security and business and strengthen the relationship. Think of the use of business information security officers who can inform specific business units about security risks and possibilities. Think also of clear arrangements or objectives that bank responsibility in business units or endorse management support.

Establishing a network of ambassadors is a way to strengthen connectivity within the organization. Strong internal stakeholder management and extensive knowledge of the business are key to a good alignment and being able to move forward together. To the business it's vital to know where in the organization the risks are situated and what kind of impact they will have. To establish this kind of ambassador network we recommend the following:

Security ambassadors community

Step 1: Know your risks

It's important to start by identifying the risks to the organization. This makes it possible to point out the processes that are prone to risks. Think ahead about events that could have negative effects on the organization or on production: what can go wrong, what are the chances that it will go wrong, what are the consequences when it goes wrong? When these risks have been identified you need to think about what kind of impact they will have on business.

Step 2: Establish management support

After identifying the risks and the impact they will have, it's important to raise awareness at management level. To be able to lessen the impact of these security risks means that security and business will have to work together closely. This collaboration is a vital starting point when it comes to working securely. Risks are located in the sphere of influence of the business and they are (partly) responsible for these risks. That's why it is of great importance that security and business work together properly. Management support is crucial in facilitating this collaboration.

Step 3: Find enthusiasts

To create support for the implementation of security measures it's important to find enthusiasts within the organization that have affinity with security. These are the people that will make the difference. They know the business very well and are able to engage others. They will contribute to the snow ball effect. Different departments or divisions within the organization will have different needs. Security on its own can not comprehend all these needs. That's why it's of great importance for security to actively approach business to create this ambassador network.

Step 4: Determine together what you have to offer

When a representative ambassador network has formed within the organization it's time to determine together what these ambassadors could offer each other. How will these ambassadors give meaning to their ambassadorship? It's essential that their role is clearly defined. What is their exact purpose and what are their responsibilities? How do you make sure these enthusiasts take full ownership of their new roles? A great start would be to organize a central kick off with all the ambassadors.

Exemplary role ambassadors

- Every ambassador is a contact person and a scout of the various business units. They have insight in recent developments of the business unit and know what is happening right now. They are the “eyes and ears” of the business unit.
- They will help out co-workers when it comes to security and are meant to set a leading example for these co-workers.
- They will help security deploy various tasks in their own department or division.

Step 5: Train the ambassadors

It’s the responsibility of security to impart knowledge to the ambassadors by means of training. Security can actively share knowledge by composing a course of different security related themes and offer this to the ambassadors. It would also be helpful to create a toolkit with security related content which the ambassadors can easily use throughout the organization.

Step 6: Set an example (activate)

When you have the right group, with the proper knowledge, you’re able to take the next step: activate business and set an example. The ambassadors can inspire business to take action on serval topics. It is important for ambassadors to identify the specific needs of the business to be able to provide security with the right kind of input and advice. In this way ambassadors will strengthen trust between security and business. During this process it’s important that there is continuous coaching from security.

Step 7: Maintain the security network

It’s important to maintain the ambassador network that has been formed. “What’s in it for them”? Make sure you don’t lose your ambassadors by creating a privileged position for them. Reward them for their accomplishments or offer them training and educational opportunities within their field of expertise. Ambassadors are usually the people in your organization that already have a great interest in security. This needs to be stimulated by continuous development of knowledge. It’s also important to share what you’ve learned within the network of ambassadors (what works at the business side and what doesn’t). Sharing these experiences will strengthen the network even further.

Ambassadors gain trust between security and business

In conclusion: security ambassadors are the ears and eyes of the organization and approach security issues from a business point of view. They are important indicators in your organization. They know what’s happening on the business side, what the needs are and where stakes either diverge or converge. They play a big role when it comes to merging security policy and reality. Maintaining this network of security ambassadors will require some effort. Support in knowledge, tools, rewards, appreciation and visible results are prerequisites for a successful network.

So, in the end it’s definitely possible to bridge the gap between business and security by deploying security ambassadors. As an organization, be openminded when it comes to critical thinkers and strengthen your security department by forming an ambassador network. This will bring about trust and strengthens the relations within the organization. And that trust is a key component when it comes to ensuring security in the organizational culture and daily operations.

About the authors:

Kim van der Veen MSc is operative at Capgemini Invent and focuses on the importance of raising cybersecurity awareness.

Evelien van Zuidam MSc specializes in human, organizational and societal issues in cybersecurity.

For more information you can contact the authors via:

kim.vander.veen@capgemini.com

Any idea of the amount of data that leaks from your organization to the internet?

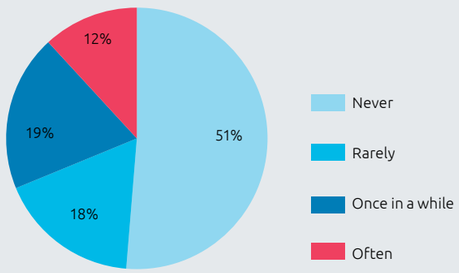
How do organizations get a grip on cloud shadow IT?

The rise of cloud shadow IT entails serious risks. Organizations need to take precautions to protect business information and to secure trust of clients and civilians.

Highlights

- **Shed light on the use of cloud applications by your employees. This is highly underestimated in most organizations.**
- **Make sure your employees are aware of the organization's security policy and the risks that accompany the use of non-approved cloud applications.**
- **Combine organizational measures (like awareness campaigns) with technological measures (like data loss prevention) to prevent data breaches.**
- **Make sure there's a continuous cyclical process in place to keep control of cloud shadow IT.**

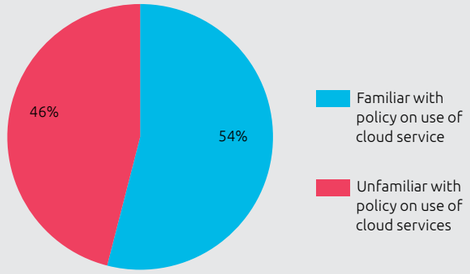
Figure 1: I save work related files (temporarily) in the cloud (e.g. through Gmail or Dropbox).



The rise of cloud shadow IT

The rise of interactive cloud applications to store, process, and share information has resulted in habituation to the ease of it. Never before has it been this easy to upload files and having someone else working on them instantly. Because of the user-friendliness, and because of the frequent use in private life, we see an increase in use of cloud applications within organizations that have not been incorporated in the formal IT and procurement processes. This is what we call cloud shadow IT. These cloud applications are not visible to IT management processes and it is difficult to get a grip on them. Organizations now face the challenge to get a grip on cloud shadow IT to protect business information and prevent data breaches.

Figure 2: I am familiar with my organization's policy on the use of cloud services.



Why is cloud shadow IT a problem?

Who does not make use of Dropbox, OneDrive or WeTransfer, to quickly exchange some corporate files? Or Evernote, to keep track of notes? Or Trello, to share tasks between project teams? Capgemini's Trends in Cybersecurity 2018 research, executed by GfK, shows that 49% of the respondents save work related data in the cloud. Cloud applications are an enrichment to daily operations but often used without involving IT. However, many employees don't realize that, as a result, they increase various risks like data breaches.

Research by Netskope shows that, on average, organizations make use of 1.022 cloud applications. A staggering 92% of these applications however, are not deemed secure enough for organizational use.[1] Given the increase of cloud applications and the organizational shift towards the cloud it's likely to expect that these numbers will grow. Additionally, research by Symantec shows that CIOs estimate the use of cloud applications in their organization between 30 and 40.[2] Much less than in reality! This illustrates that organizations often have insufficient understanding of cloud shadow IT and the risks they bring along.

Usually a software application is approved for data processing up to a certain level of classification and is monitored to see if it complies with the data protection policy of the organization. Depending on the level of classification (e.g. public, confidential or state secret) and security policies that apply security measures are put in place. This should also happen for cloud applications but doesn't happen for cloud shadow applications. In addition to this, only half of the Trends in Cybersecurity 2018 respondents are familiar with their organization's security policy. Crucial questions go unanswered: is data encrypted, and if so, by which encryption method and who manages the key? Who has access to data? Where is data stored? As a result, security measures like logical access and encrypting data are not or insufficiently applied.

Consequently, this means that possibly sensitive business and personal data is stored on the internet without being able to control this data. What are the perceivable risks and how do they impact the organization? We've have outlined the most occurring risks:

- **Chance of data breaches because many cloud applications do not comply with the internal security policy of the organization.** Most cloud applications do not necessarily live up to the security demands your organization sets toward IT systems. When it comes to shadow cloud IT looking into these security measures is usually skipped. With contracted cloud applications organizations sometimes have some input when it comes to securing them but with noncontracted applications there is hardly anything that can be done to secure them in the right way. Some free cloud services even stipulate in their terms and conditions that all data becomes property of the provider of that cloud service. This means that by using these services, as an organization you lose intellectual ownership of your data.

- **Business information is stored at many unknown locations.** Because cloud shadow IT is brought to use outside of the formal IT processes, organization have a hard time gaining insight in where their data is being send to. Increased use of cloud shadow IT means that there are even more places where business information gets stored. In addition to this, most cloud applications make use of third party infrastructure. For instance, a cloud application that runs on Amazon Web Services infrastructure. End-users are often unaware of this third-party infrastructure and that makes it even harder to keep track of what kind of data is being stored and who has access to this data.

What is cloud shadow IT?

The concept of "cloud shadow IT" is used to categorize all cloud applications that are used but have not been incorporated in the formal IT and procurement processes of the organization. Examples are Dropbox, sharing services like WeTransfer and online converters to convert Word files to PDF.

[1] **Netskope Cloud report September 2017**
[2] **Symantec 1H 2017 Shadow Data Report**

- **Violation of legislation and regulation leads to compliance issues.** In Europe we have strict legislation concerning the protection of personal data. Organizations have to be able to prove that they have implemented sufficient security measures to prevent data breaches. With the enforcement of the General Data Protection Regulation (GDPR) and the extensive amount of personal data that is processed, this is a key focus for most organizations. In addition, organizations have to compose and keep track of a register of data processing activities. To do so, it's important to know where personal data is being stored. If, for efficiency reasons, employees make use of various (free) cloud applications this might lead to violation of legislation and regulation. Which in turn could lead to potentially major fines.

- **Increased costs due to lack of central procurement of cloud applications.** According to Skyhigh Networks' research organizations, on average, make us of 210 cloud applications for online collaboration and 76 cloud applications for online storage and sharing of files. Chances are that these cloud applications overlap and that the number can be reduced tremendously. By centrally procuring cloud applications the organization can make use of bulk prizing and volume discounts. This can help reduce costs significantly.

Keep track of cloud shadow IT

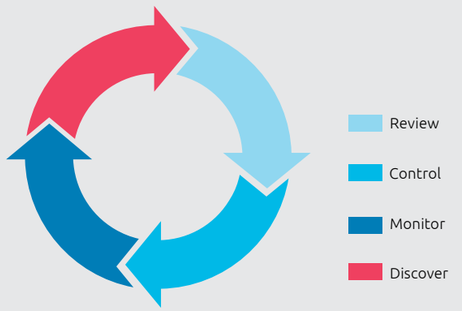
Discover – Gain insight in cloud shadow IT

In order to get a grip on cloud shadow IT it's important for organizations to gain insight in cloud applications that are used internally. There are several tools available to help you along. A cloud access security broker can monitor network traffic between your corporate network and the internet. It can also generate overviews and statistics of how many people use certain cloud applications and how much data gets send there. These kinds of tools usually provide a database with characteristics and risk profiles per cloud application, making gaining insight in possible liabilities quicker and easier.

Review – Evaluating cloud applications

After gaining insight in the use of cloud applications it's important for organizations to determine which ones are or need to be approved for use and which ones are not. Every cloud application needs to be carefully considered by means of risk analysis. Risk aspects to take into consideration are: the amount of data that flows from the organization to the cloud application, the reliability of the cloud service provider, is the cloud application used for business of private purposes, etc. As a result, cloud applications can be divided in three categories: explicit approval for cloud applications that are used for business purposes, condonement of cloud applications that are predominantly used for private purposes and block cloud applications that impose a risk. This policy needs to be dispersed to everyone within the organization, for example though awareness campaigns.

Figure 3: Process of keeping track of cloud shadow IT.



Control – Putting in place the required security precautions

As soon as it's clear which cloud applications are approved security measures can be determined. This is also the time to see if there might be any overlap between cloud applications. Reducing the overlap – and thus bringing down the number of cloud applications – will not only reduce costs but also diminish chances of data breaches. The next step will be to implement an active access policy to protect business information, that is now stored outside the organization, against unauthorized access and connect cloud applications to existing monitoring software (like SIEM) in order to detect deviant behavior. Another precaution that can be taken is to completely block access to high risk cloud applications. Some cloud applications entail such high risks (e.g. an unencrypted connection, terms and conditions that transfer intellectual ownership, etc.) that it would be wise to just deny access to them. Crucial in this process is to keep your employees informed about the risks that (the use of) cloud applications entail.

Monitor – Regular review of use

Now it's important to regularly review the use of cloud applications. Especially at the beginning it would be recommendable to go through this process on a monthly basis. This helps recognition of new cloud applications in a timely manner. If new cloud applications are detected follow the same process: from risk analysis to determining the right security precautions. In addition, there are tools that can help monitor deviant behavior; uploading of much more data than average to a cloud application that is condoned for private use could indicate a data breach.

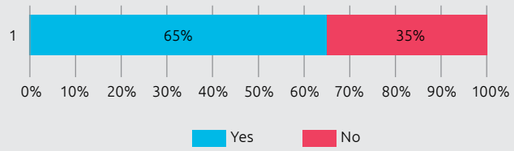
In conclusion

It is impossible to imagine a contemporary organization without cloud applications. That is why it is of utmost importance to gain insight in the use of all cloud applications within your organization to determine the risks that they bring along. 65% of the Trends in Cybersecurity 2018 research respondents say that they're familiar with the risks of saving work related files to cloud applications that have not formally been approved for use.

Despite this familiarity we see that there are, on average, a 1.000 cloud applications in use within organizations. Most of these fall outside the range of formal IT management processes.

Considering the increase in cloud applications we expect to see that this number will only rise over the next 5 years. In order to maintain the trust of clients and/or civilians and to avoid violation of legislation and regulation, organizations now have to rise to the occasion and prevent data breaches!

Figure 4: 51% of respondents save work related files (temporarily) to the cloud. 65% van these are familiar with the accompanying risks.



About the authors:

Manon Stolte MSc and Michail Theuns MSc are, respectively, senior cybersecurity consultant and managing cybersecurity consultant at Capgemini. They both focus on cybersecurity and privacy and advice clients on how to secure their prized possessions.

For more information you can contact the authors via:

manon.stolte@capgemini.com

michail.theuns@capgemini.com

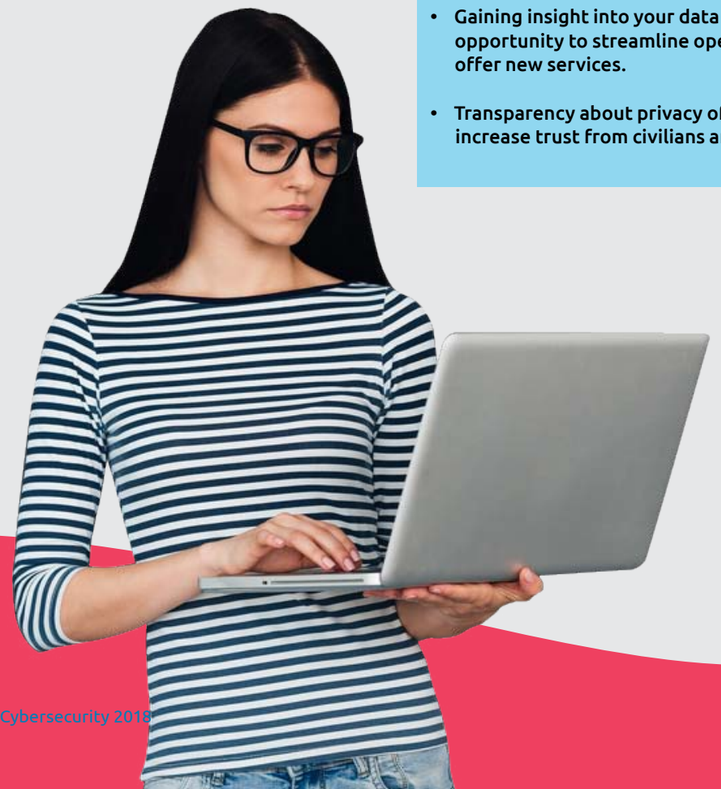
Goldilocks in privacy land

How can organizations benefit from the General Data Protection Regulation (GDPR)?

Many organizations perceive the implementation of the new privacy legislation GDPR as an expensive compliance exercise. That is unfortunate because this new law presents an opportunity to gain better insight in the data flows of an organization. Better insight into data flows allows for more effective collection and use of information to increase the value of an organization and lower costs. What other opportunities does this legislation provide? And how can organizations turn it to their advantage?

Highlights

- **New privacy legislation GDPR and ePrivacy directive offer organizations the opportunity to distinguish themselves.**
- **Going beyond the compliance conundrum: GDPR provides the opportunity to improve your information management.**
- **Gaining insight into your data flows gives you the opportunity to streamline operations, reduce costs and offer new services.**
- **Transparency about privacy offers you a chance to increase trust from civilians and clients.**



The implementation of the General Data Protection Regulation (GDPR) and the upcoming ePrivacy directive have shaken government and corporation alike. There is a pervading perception that anyone handling personal data must overturn their entire operation to prevent hefty fines. Unsurprisingly, many organizations view the implementation of the GDPR as a costly "must", imposed by Brussels.

However, these organizations are missing out on a big opportunity. Besides furthering more privacy and data protection, both the GDPR and ePrivacy directive offer opportunities to improve both general information management and internal processes. Especially for organizations often dealing with sensitive information, such as municipalities and government bodies, implementation of the GDPR is a big deal. Numerous incidents involving data breaches and malpractice in these institutions have eroded citizen trust over the years.[1]

The new privacy legislation compels organizations to be transparent about the data they collect and to use it responsibly. It also provides better insight in data collection processes and gives the organization the opportunity to increase trust from civilians and clients.

In the fairytale "Goldilocks and the three bears" Goldilocks slips into the house of three bears and tastes their porridge. One is too hot, one is too cold, but one, one is just right. This "Goldilocks standard" can also be applied to the implementation of the GDPR and (later on) the ePrivacy directive. Organizations should not merely stick to the high-level paperwork, but they should not impose lumbering bureaucratic structures either.

May 25th, 2018

By now everyone will be aware that the GDPR has been enforced. The overview below summarizes the GDPR and the requirements it places on organizations, in ten questions. The law has been in place since 2016 but was only enforced in 2018, to give organizations time to meet the requirements of the law.

The GDPR in 10 questions:

- Who's personal data do you process?
- What personal data do you process?
- For what purpose do you process personal data?
- For whom do you process personal data? Who processes it?
- What types of personal data are prone to risk?
- What precautions did you take to protect personal data?
- Can data breaches be reported and managed?
- Can you provide information about your processing activities to users and regulators?
- Are you able to provide individuals their rights?
- Do you limit the collection, processing and storing of personal data to set objectives and periods of time?

[1] https://www.omroepgelderland.nl/nieuws/2126640/Persoonsgegevens-op-straat-door-datalekken-bij-Gelderse-gemeenten
https://www.omroepwest.nl/nieuws/3529773/VVD-bezorgd-over-datalek-gemeente-Den-Haag
https://nos.nl/artikel/2219565-gezochte-politiemol-mark-m-meldt-zich-bij-politie-in-roermond.html
https://www.omroepwest.nl/nieuws/3583192/Politiemol-uit-Zoetermeer-lekte-informatie-over-31-mensen-en-meerdere-kentekens
https://www.ad.nl/gouda/persoonsgegevens-inwoners-krimpenerwaard-gelekt~a98485e8/
https://www.rtlnieuws.nl/nederland/gevoelige-gegevens-1800-kwetsbare-kinderen-op-straat
https://rejo.zenger.nl/vizier/gevoelige-gegevens-onveilig-bij-politie/
https://nos.nl/artikel/2004565-tientallen-geheime-documenten-politie-op-straat.html
https://decorrespondent.nl/3734/nieuws-de-politie-blijkt-op-grote-schaal-de-wet-te-overtreden/510916939412-7be7c192

A direct cause of improving data protection through all of Europe is the (perceived) derailment of data collection by various organizations. Think, for instance, about U.S. tech giants like Facebook and Google who widely collect data from their users. But don't forget about governments, municipalities and intelligence services that collect and store (too) much personal data for undefined purposes.[2] Some of these organizations don't shy away from utilizing data collected by tech giants either. The NSA famously had direct access to their data.[3] The National Police also makes use of similar information sources and reaches out to Microsoft[4], Apple[5] and tax authorities[6] regularly. Even more legislation is applicable to data protection when it comes to the security domain.

ePrivacy directive

In addition to the GDPR there will be an ePrivacy directive to replace the current guidelines. This directive complements the GDPR and places additional requirements unto data collection by means of marketing channels and the protection of communication like email, cookies and telemarketing. Replacing the Guideline from 2002, this Directive will align legislation across Europe, replacing local legislation, like the Dutch cookie law. The span of the Directive will also increase because Over The Top (OTT) services like WhatsApp, Snapchat, Netflix and the Internet of Things (IoT) will now have to adhere to this legislation as well.

The GDPR has been implemented on May 25th, 2018. No date has been set for the implementation of the ePrivacy Directive. This date is a first milestone. Regulators will demand action from organizations that lag behind. Organizations that have already implemented the GDPR will have to meet the requirement of "continuous improvement" of data protection.

Minimal or maximal?

The new privacy legislation has been interpreted differently across organizations. Thinking of Goldilocks: we take a look at two of these approaches; minimal and maximal implementation.

Minimal

Minimal implementation focuses on compliance ("ticking all the boxes"). In this approach organizations aim to record all necessary aspects in an array of policy documents thus creating a "paper tiger". All requirements are met on paper, but they do not have any consequences in the real world, rendering them ineffective. To have a data breach policy is great. But if your organization actually encounters a breach and no one knows how to handle, no one will be able to limit the consequences.

By choosing the minimal approach, the organization will primarily experience costs. In the short term these costs will be relatively low because of the limited changes made. Work processes and existing systems are barely affected. However, these organizations will miss out on the benefits and opportunities that this new legislation has to offer. Ultimately, this minimal approach could even lead to reputational damage when it turns out that the organization does not make good on its word. So in short; some costs, hardly any benefits and little insight in financial as well as reputational damages.

Maximal

A maximalist approach takes privacy into consideration throughout the entire company structure (privacy by design). This way the organization understands the risks that come along with information processing, is able to process request from those involved immediately and has live insight into the information landscape, from HR to Marketing. This approach ensures a transparent organization and enables compliance towards regulators and clients.

[2] For example, see: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/

[3] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Network%20front:network-front%20main-2%20Special%20
https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story

[4] https://blog.elcomsoft.com/2017/01/government-request-reports-google-apple-and-microsoft/

[5] https://www.security.nl/posting/468197/Politie+vroeg+Apple+om+infor
http://images.apple.com/legal/privacy/transparency/requests-2015-H2-en.pdf

[6] https://decorrespondent.nl/1841/politie-en-inlichtingendiensten-kunnen-via-een-achterdeur-bij-gegevens-van-de-belastingdienst/56621796-863e993b
https://tweakers.net/nieuws/124773/aantal-opvragingen-door-opsporingsdiensten-bij-providers-daalt-licht.html

Minimal implementation	Maximal implementation
• Compliance • Short term: low costs • Clear overview of costs and benefits • Regulator as risk factor • Privacy as potential risk (being unable to meet the accountability demand) • Hardly any impact in day to day business	• Privacy as a positive denominator in business operations • Far stretching data protection • Short term: high costs • View on future benefits: limited • Good relations with regulators • Privacy as an advantage when it comes to clients • Big impact on processes (opportunities to slim down and reduce costs) • At risk to get stuck in formalities

However, by implementing this maximalist approach there is much more to gain than just transparency and accountability. By not just focusing on internal data protection as legislation dictates, but by making it part of company structure you create the opportunity to increase the value of data for your organization. The downside to this approach is that it is costly and has limited short term benefits. In the long run however, this implementation will generate many opportunities by fostering a more structural understanding of data flows within the organization. This, in turn, will make it possible to streamline procedures and reduce costs. In addition, a maximalist approach will bring about a culture in which data protection considerations are taken into account on all levels and in all processes of the organization. This reduces the chance of incidents. As part of the (communication) strategy, it could also regain or strengthen civilian trust in organizations.

Or somewhere in the middle? The three bears

If we take an honest look at the way GDPR legislation is implemented, we have to agree that most organizations reach for the minimalist approach. Everyone is looking at everyone else. What are others doing? How will regulators react if organizations fall short?

As far as we're concerned the ideal approach is somewhere in the middle; the so-called Goldilocks standard. Don't do too much, but don't do too little either. This middle ground approach offers opportunities from the maximalist approach without getting stuck in formalities. Read on for some outlines on this middle ground approach.

Which components could make up a middle ground approach?

An approach that focuses on privacy as a positive denominator will initially bring along higher costs. Investments will have to be made to get a grip on data and data flow. This will however also bring about innovation which in the long run could be a significant cost reduction.

1. Overview of data and data flow

The GDPR requires all organizations to keep track of where they store data. This means that organizations will have to go through all the information they own. This could lead to valuable insights. Most organizations have little insight into their information landscape, whether it is about personal data or data in general. It is often unclear where data is stored, what kind of data is stored and who the owners are. This subsequently leads to even more data collection which in the end is unnecessary and brings along unwanted risks. Legacy systems, growing connections between databases and exchanging data between third parties all complicate gaining insight from data and ultimately hamper effective value generation for the business. By making use of data discovery analytics dataflows can be mapped. This is not only useful when it comes to personal data but to any type of information an organization may hold. In the end this can form the basis of simplifying the application landscape on all organizational levels.

2. Simplify the application landscape

The new legislation also establishes requirements when it comes to applications. One of the most important requirements is to delete data when there is no longer a use for it (there is no contract nor legal justification to store it). It sometimes proves to be difficult to remove data from older applications. This has led to accelerated phasing out of older applications. These forced innovations can bring about certain advantages (the so-called headlong rush); organizations that have been "stuck in the past" are now gently nudged onto the road of innovation.

3. Improved data protection

The GDPR requirements help organizations to get an overview of their information landscape and the processes that bring along high risks. This gives organizations the opportunity to make improvements when it comes to protecting their data. In recent years organizations have come to realize that information is their greatest asset but they're not quite there yet when it comes to protecting this data. This forced evaluation of personal data protection policies also forces organizations to think about data protection in general and risk management in a broader sense. Especially the GDPR requirements concerning crisis and risk management add clear organizational (mostly technological) measures to the conventional range of possibilities. A proper way of dealing with incidents is also key to intellectual freedom and fraud.

4. Building trust

A well established and clearly communicated privacy policy can resolve concerns with consumers as well as employees. The GfK research that forms the foundation of Trends in Security indicates that 80% of respondents believe that more regulation is needed to regarding the collection and use of data by tech giants like Google, Facebook and WhatsApp. Loss of trust is a real risk for organizations. Honest and proactive communication about policy and incidents can help resolve concerns that consumers may have and, in the end, even help convince them to choose you over the competition

All these components have one thing in common; they comply with the requirements set in the GDPR. But they're also connected to tangible objectives and improvements for organizations. You are going to have to swallow that GDPR porridge, one way or another. So, when you do, make sure that the temperature is to your taste.

A bright future for privacy

Somewhere between a minimalist approach that focuses on compliance and a maximalist approach that ritualizes privacy, there is a middle ground. At the core of this middle ground approach lie a clear baseline, solid principles, substantiated insights and transparent communications concerning privacy policies. From current standings, where organizations simply absorb data and endure legislation to a future where organizations grab control over the way the purposely collect high quality data.

About the authors:

Melle van den Berg is senior consultant at Capgemini Invent. He advises clients on how to effectively implement GDPR.

Ton Slewe MBA CISSP is principal consultant at Capgemini. He focuses on cybersecurity issues in public and private organizations.

Alice van de Bovenkamp is cybersecurity and privacy consultant and part of Capgemini's Public Order & Security division.

For more information you can contact the authors via:
melle.vanden.berg@capgemini.com

alice.vande.bovenkamp@capgemini.com

ton.slewe@capgemini.com

Strong universal authentication: increasing trust in electronic services

When is your organization going to utilize strong authentication to better protect your clients and employees?

Access control is essential to secure electronic services. Service providers need to know who is “on the other side of the line”. User identification is also known as authentication. Current login tools are not sufficiently secure to prevent fraud, abuse, identity theft or reputational damage. As a result, trust in electronic services is decreasing. Luckily, there is a better way: universal 2nd factor authentication (U2F). The development of U2F is very important to the (public) safety domain. Major browsers like Google Chrome, Opera, and Firefox have built-in support for U2F since 2017. Tech companies including Google and Facebook have implemented U2F for their employees as well as their clients. When is your organization going to utilize U2F and provide better protection for your clients and employees?

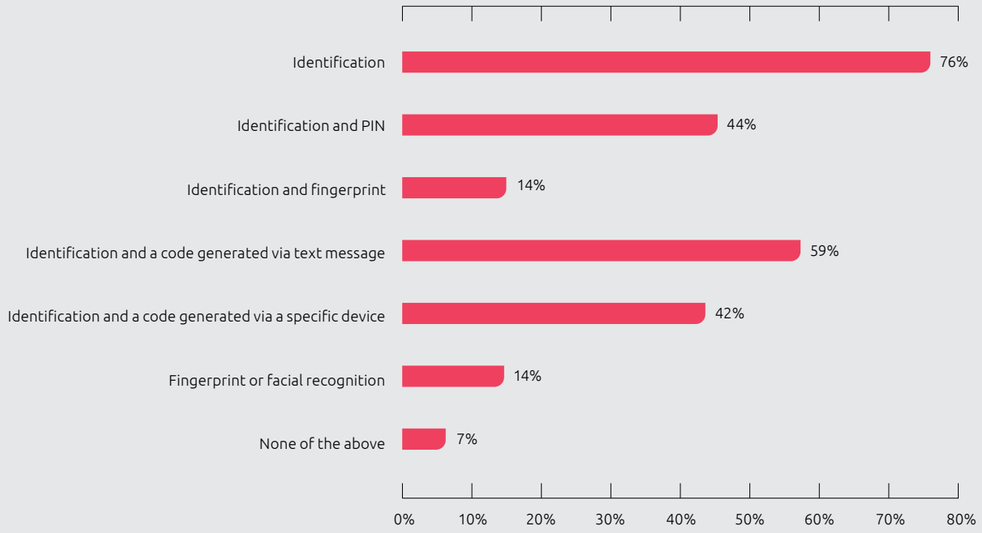
Highlights

- **Current login methods are not sufficiently secure and lack user-friendliness.**
- **This makes electronic services vulnerable to fraud.**
- **Universal 2nd factor authentication (U2F) is a secure alternative that can prevent fraud. U2F is based on an open standard and is user-friendly.**
- **The U2F security key is universal and can be used to login with multiple service providers.**
- **Service providers can increase security of their services without big investments.**

Persistent leakage of passwords

In the last few years, there have been several data breaches that generated a lot of media attention. In 2017, a file was discovered on the Dark Web containing 1.7 billion pieces of personal data. Apart from the account names that were leaked, 17% of the data consisted of unencrypted passwords. The data seemed to come from multiple electronic service providers including LinkedIn, Netflix, MySpace and the less well-known Last.FM. Earlier, LinkedIn was hacked due to a flaw in their information security and 164 million accounts were made public. Passwords were easily decrypted, allowing wrongdoers to gain access to other services that were protected by the same credentials. On top of that, a large number of email addresses was uncovered and immediately targeted by banking malware. The service providers mentioned above were not the only ones to have struggled with security breaches. Research conducted by GfK in the Netherlands in 2018 points out that a relatively large group of people still use weak login methods, as shown in the figure below.

Which login methods do you privately use?



Flaws of current methods

There are many different authentication methods. Password-based authentication, for instance, is still widely used. It does, however, have its vulnerabilities. Many people tend to use the same password for different accounts. Once that password becomes public due to a data breach at a certain provider, other services can be exposed to abuse as well. Cybercriminals often make use of phishing, a technique to lure people into entering account names and passwords on a fake website. On top of that, the passwords themselves are often flawed in the sense that they are usually uncomplicated and easy to guess. Plus, people tend to forget their passwords and are forced to write them down, exposing themselves to further risk in the process. In some cases, a second channel may be required by the environment, in order to provide further security. A randomly generated code that is distributed through a text message is such an example. Unfortunately, text messages are no longer considered sufficiently secure.

A better, safer login method is 2nd factor authentication (2FA) or multi factor authentication (MFA). These types of authentication are based on something you know, something you have or something you are to confirm the user's identity. As an example, specific devices are used in the banking sector to generate a specific code. You place your bank card in the device and enter your PIN. The device then generates a code and you must use this code to securely login to the banking website. This form of authentication is much more secure, because the generated code can only be used once. However, every service provider has its own device. Logging into multiple websites, then, may require multiple devices – a rather inconvenient state of affairs.

Instead of a PIN, it is also possible to use biometric properties like fingerprints or facial recognition. The use of biometric properties is much easier, but sometimes biometric sensors are easily manipulated. What are the consequences if someone succeeds in copying your biometric properties?

Finding a better way: U2F

Relatively new to the field is universal 2nd factor authentication (U2F). U2F is a standardized, universal security token that can be connected to, amongst others, a USB port. U2F is developed by FIDO Alliance. Members of the FIDO Alliance include Google, AMEX, ING Bank and Intel. This form of authentication has some major advantages. For service providers U2F is easily implemented through a cloud solution (as-a-service). There is also a big advantage for the user: U2F is very user-friendly. After a one-time registration with the service provider, there is only one thing left to do: insert the security key into the USB port and press the button. FIDO 2.0 can also be used on smartphones via Near Field Communication (NFC). Tap the security key on your smartphone and you are good to go.

You can easily switch from service provider and connect the security key to a different account. U2F also has some security benefits. The cryptography is based on public key encryption and the secret key cannot be detached from the physical security key. Biometric properties are also permanently bound to the security key.

A certification program has been established to guarantee key interoperability and security. The security of keys is evaluated through several levels of certification. To facilitate the process, several accredited laboratories have been established. Hundreds of security keys have already been certified since the inception of the method.

U2F has been designed to counter phishing and man-in-the-middle attacks as well. This improvement in security will increase trust in electronic services. The code that is generated through U2F, can only be used to login to one single specific website. The domain name is incorporated into the U2F security key's cryptographic calculation. Because the authenticity of the security key can be verified, service providers are able to enforce the use of a specific security key. Due to these security advantages, the risk of login information abuse is mitigated, as is the risk of potential resulting damage.

Just like any other form of authentication, U2F has some downsides. The security key is not protected against physical theft and could be stolen. To (mis)use the stolen key however, you would still need the username and password. If the key were to be lost or damaged, you would need an alternative login method. A backup key, kept at a secure place, could be an option. If the security key is lost, it could take a lot of time to block it, especially when it is used to login to multiple electronically services.

Alliance of trust

FIDO Alliance, including Google, Facebook, and Microsoft, is further developing the U2F standard. The aim is for clients to use the security key to login to multiple service providers. Some FIDO Alliance members have implemented the security key for their employees as well as their clients. Google's support department estimates that switching to U2F has already saved them thousands of hours in servicedesk support. One-time passwords (OTPs) took up a lot more time. As a result, U2F is not only a more secure login method, it is also less expensive than current OTP methods.

The U.K. government is also embracing the use of U2F. They are providing their citizens with the opportunity to sign up for the GOV.UK Verify program. By using a U2F security key, citizens can gain access to several public services like tax authorities and retirement services. Other services are expected to follow shortly.

Further development of authentication standards and security keys

In their search for more secure login methods, a growing number of service providers will embrace this universal standard. We expect suppliers to get on board as well. Service providers will further facilitate the use of U2F/FIDO 2.0.

Part of FIDO 2.0 is the Universal Authentication Framework (UAF). UAF is developed for smartphones and uses a PIN or fingerprint as login method.

Microsoft, just like other tech companies, is developing a passwordless login method: Windows Hello. This new feature uses, in addition to the security key, biometric properties or a PIN as second factor. FIDO 2.0 support in Microsoft Edge, through Windows Hello, would mean that users are able to login to their devices as well as services providers without using complicated passwords.

Other security keys are able to show either the websites that you have accessed or the transaction details. This confirms that you have actually accessed the right website. There are also tokens that use biometric properties (fingerprints) when enabling the security key. This way, only the rightful owner is able to use the key.

Key to the future

U2F is a safe, universal, and easily implementable solution to help electronic services become more secure. Large tech companies have embraced this approach, both for their employees and clients. Service providers are realizing that current login methods are not sufficiently secure and are in search of a simple and secure alternative. We expect to see even more organizations embracing the U2F approach, both inside and outside the safety domain.

About the authors:

Ton Slewe MBA CISSP is principal consultant at Capgemini. He focuses on cybersecurity issues in public and private organizations. Arjen Hartog is senior consultant at Capgemini. He focuses on cybersecurity issues. Norbert van Adrichem is senior consultant at Capgemini. He brings together business and technique on cybersecurity.

For more information you can contact the authors via:

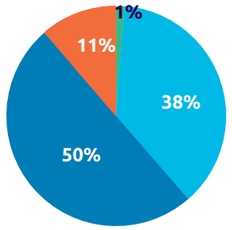
ton.slewe@capgemini.com

arjen.hartog@capgemini.com

norbert.van.adrichem@capgemini.com

Security

Do you ever feel unsafe?



Trust in the **digital society** is divided. 19% have a lot of confidence and 23% have very little.

64% consider a **digital attack** more likely than a physical attack.

The government is insufficiently prepared for a **cyberwar,** according to 60% of the Dutch. According to 52% this also applies to companies.

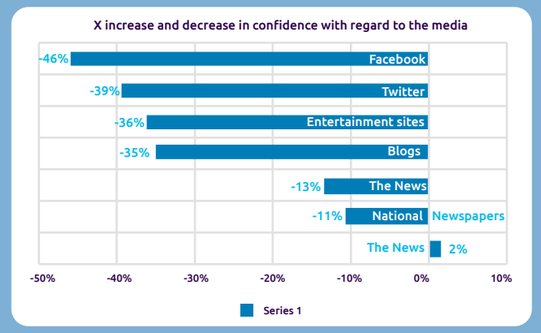
67% think that **foreign states** influence us.

74% believe that fighting **cybercrime** should become top priority. (People aged 65+ agree most strongly on this)

82% believe that the **government** should do more to increase digital security.

Media: trust is decreasing

Trust in the **media** has decreased, except for trust in the news (+ 2%).



62% regard the spread of **fake news** as a **threat to security.** Only 10% disagree.

41% feel that t**hreats through social media** are just as serious as in real life: more often women and more often 65+.

Compared to 5 years ago, 47% see a less clear **distinction** between real and false **facts**.

Detection: digital and civilian

87% believe that civilians **are allowed to support the police** in criminal offences. People are more cautious about support in serious crimes (5%).

63% are in favor of the use of **social media** by the government to **detect crime**, 8% is against.

54% find **algorithms** suitable for the detection of digital crime on social media.

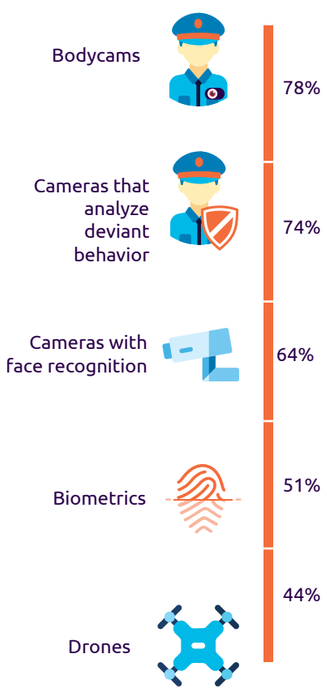
In a **regional calamity**, people mainly search for information on the internet (81%), television (68%), and radio (54%).

Digital development

Only 9% do not feel comfortable with the growing number of **cameras in public areas**.

People are **positive** about **digital tools** to increase security. Trust in the latest security techniques is lagging behind against traditional methods of identification.

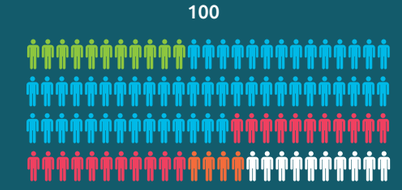
61% are concerned about the security of **IoT devices.**



Internet behavior

1 in 10 people never change their password!

Never	11%
Sometimes (every year)	53%
Regularly (every 3 to 6 months)	22%
Often (every month)	4%
Only when I am obliged to do so	10%



31% occasionally/often (temporarily) store work-related documents in the cloud. Of this, 54% is familiar with the **policy** and 65% is familiar with the **risks.**

Traditional login methods are still preferred. Single identification (76%) or through SMS (59%) versus fingerprint (14%) and face recognition (14%).

Research conducted by GfK, N = 1000.

Publications

In addition to our Trends in Cybersecurity report, we publish other reports, surveys and white papers that may be relevant to you.

Below you will find a brief overview.
A complete overview of our publications can be found at: www.capgemini.com/nl-nl

Digital Transformation Review 10: The Digital Culture Journey: all on board

Digital technologies allow organizations to reinvent themselves, transforming the core of the business and finding and exploiting new sources of value.

However, many organizations are struggling to reinvent themselves because they run into a significant culture barrier. Our research shows that culture is the number one barrier to digital transformation. This edition of the Digital Transformation Review focuses on this critical, but neglected, topic:

- How are large and traditional organizations tackling the delicate issue of digital culture?
- What do digital-native firms do differently when it comes to digital culture?
- What advice do leading academics have for organizations attempting to get the digital culture change right?

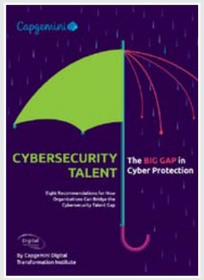
We share the insights of key leaders and experts on this topic, representing the views of traditional companies, academics, and the Silicon Valley.

www.capgemini.com/resources/digital-transformation-review-10/

Digital Transformation Review 11: Artificial Intelligence Decoded

The 11th edition of Capgemini's flagship publication, the Digital Transformation Review, focuses on Artificial Intelligence (AI). It's a topic of high interest to both consumers and enterprises. This edition presents a nuanced perspective on AI to help cut through the hype and fog.

www.capgemini.com/service/digital-transformation-review-11-artificial-intelligence-decoded/



Cybersecurity talent - the big gap in cyber protection

This research focuses on cybersecurity talent, a skill set that is in low supply and in high demand. We have surveyed over 1,200 senior executives and front-line employees. It includes interviews with key experts like academics, cybersecurity associations, and the recruitment sector. We have also analyzed social media sentiment of around 8,400 current and former employees at 53 cybersecurity firms.

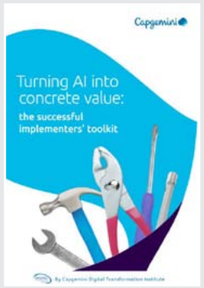
www.capgemini.com/resources/cybersecurity-talent-gap/

The discipline of innovation

This research undertaken by the Digital Transformation Institute, is an attempt to understanding the gap between the creation of innovation centers and real innovation that results from this, and to explore ways to bridge this gap. As part of a series of reports focused on innovation centers, this edition looks to answer the following questions:

- Are organizations becoming more innovative as a result of their investments in innovation centers?
- What is holding organizations back from achieving innovation maturity and turning investment into results?
- How can organizations maximize the value from their innovation efforts and investment?

www.capgemini.com/resources/the-discipline-of-innovation/



Turning AI into concrete value: the successful implementers' toolkit

A Capgemini study of nearly 1,000 organizations implementing Artificial Intelligence highlights the growth opportunity of AI and counters fears that AI will cause massive job losses in the short term. This research is a pragmatic guide to help organizations in their AI investment decisions. We analyzed more than 50 AI use cases regarding their adoption, complexity, and benefits. We surveyed senior executives from nearly 1,000 organizations around the world that are already implementing AI. We also spoke to academics - as well as AI-focused executives at global companies, startups, and vendors to investigate all that AI has to offer.

www.capgemini.com/resources/turning-ai-into-concrete-value/

Blogs

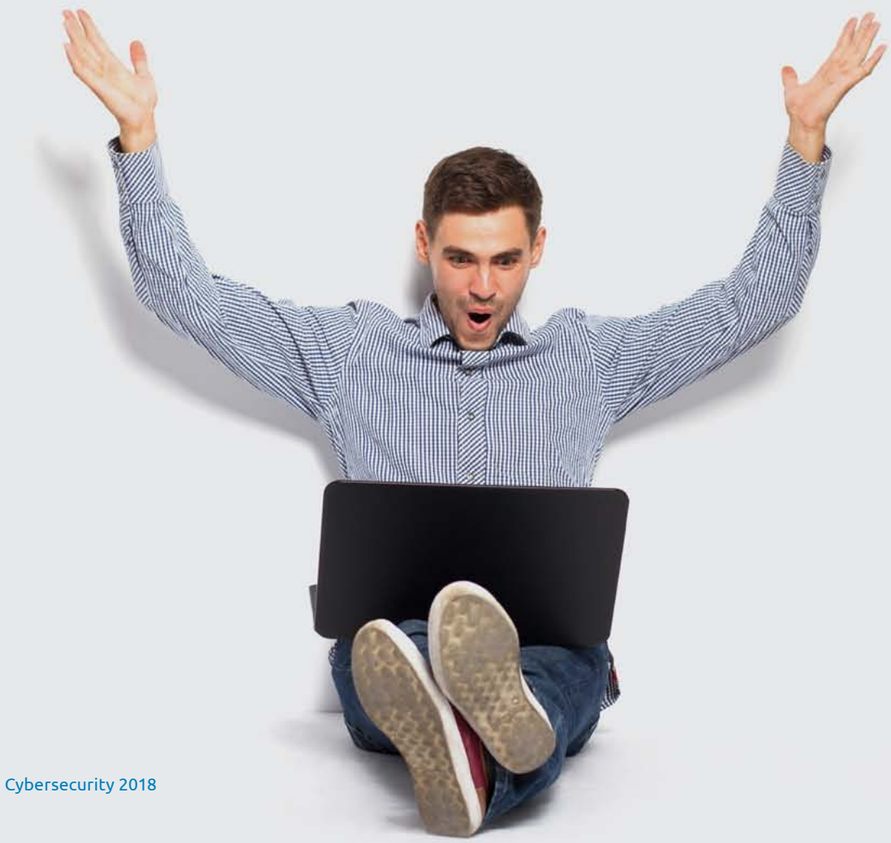
Trends in Cybersecurity blogs

Our experts and thought leaders are daily engaged in organizations, processes, policies, and management in the entire security domain. Their blogs are frequently publicized on our Trends in Security website. The blogs can help you keep up to date with the latest insights, trends and developments within the security domain.

Go to the Trends in Security blogs at: www.trendsinveiligheid.nl

All general Capgemini blogs via:

Netherlands: www.capgemini.com/nl-nl/blogs/
Global: www.capgemini.com/blogs/



Colophon

Erik Hoorweg
Gerard-Pieter Borren
Paul Visser
Edwin Kok
Erik Staffeleu
Kim van der Veen
Sjoerd van Veen
Thomas de Klerk
Jules Jongerius (intern)

Capgemini Nederland B.V.
PO 2575 – 3500 GN Utrecht
phone: +31 30 689 00 00
email: trendsinveiligheid.nl@capgemini.com
www.trendsinveiligheid.nl

Advice, design, and production: Marketing & Communication, Joke Achterberg, Trina Nandi, Syan Ghosh

Photography: Schutterstock

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2017 global revenues of EUR 12.8 billion.

Visit us at

www.capgemini.com/nl-nl

For more details contact:

Capgemini Nederland B.V.
P.O. Box 2575, 3500 GN Utrecht
Tel. + 31 30 689 00 00
www.capgemini.com/nl-nl

People matter, results count.

IN/1B-112.18