Capgemini

Trends in Cybersecurity 2017-2018

Trends in Cybersecurity
2017-2018

Preface

The world is connected. The internet has connected people, organization and devices. The speed at which these connections are made is enormous. Soon everything and everyone will be connected via the Internet. It is clear that far-reaching digitalization is going to change almost every aspect of society. Not only in the Netherlands but worldwide. Organizations and people will adapt... or not.

In all sectors, the upcoming digitization places societies for profound dilemmas, challenges and opportunities. Technological development can open roads to more prosperity, health, well-being, security and sustainability - but only if we ensure that new technologies, people and societies reinforce each other.

Connected organizations, people and devices offer new opportunities, such as better services to customers and citizens through smart data sharing. Or more public safety through smart cameras connected to databases and automatic face recognition. We also see opportunities to anticipate risks in terms of safety and viability, for example by proactively monitoring social media.

Increased connectivity of devices and systems also entails new vulnerabilities, such as insufficient control over user identity, inadequate authorizations, non-registration of equipment, lack of a secure update mechanism, or the use of standard passwords. In addition, some new technologies may have a major impact on the privacy of individuals. If Dutch society is to become more

resilient, the Ministry of Defense has to play a bigger role. After all, our digital society is fully connected to foreign countries.

Organizations must dwell upon the fact that they are part of a digital chain for the development or delivery of products and services. Vulnerabilities in one of the parts in the network can lead to risks to other parts. The described technological changes also ensure alterations in the way of working in the security domain. It requires agility of organizations and new organizational principles. Organizational principles in which the focus is on the purpose. Away from a system world. Back to a social environment in which trust, quality, time, attention and freedom of choice are central.

How do you cope with these new developments? We hope this edition of Trends in Security will provide you with concrete tools.

Enjoy reading
On behalf of Capgemini Nederland B.V. and Capgemini Consulting.

Erik Hoorweg | Paul Visser

Table of Contents

Management Summary Trends in Security 2017

That digitization is changing our society is, in itself, nothing new. The speed of change, however, is often underestimated. Technology is not evolving linearly, but exponentially, and our brains are not suited to think exponentially. Some idea of this speed, however, is necessary if we want to understand the significance of the current trends in our society. This involves an understanding of the connections that are driven by the developments:

- Connections between devices
- Connections between enormous amounts of data
- Connections between organizations
- Connections between government and citizen
- Connections between privacy and security

This edition of Trends in Security provides in-depth discussions of these connections.

The exponential growth of technological possibilities represents enormous opportunities for industries as well as the consumers, but especially for the public sector, as a means to boost public safety.

Figure 1: More than half of the Dutch people are worried about the increase in insufficiently secure technologies that are connected through the Internet.

To what extent do you agree with the following statement?

I am worried about the growing number of insufficiently secure technologies that are connected through the Internet (e.g. thermostats, smart meters, alarms, smart televisions, etc.).

A society - where everyday objects are fitted with interconnected sensors - has an unprecedented source of data at its disposal. If these sensors are specifically concerned with safety and security, they are part of the so-called Internet of Safety and Security Things (IoSST). IoSST represents opportunities for the enforcement of public order and safety. As an example, through the automatic combination and analysis of data concerning public spaces, we are able to anticipate risks to safety and liveability. Dutch people, on the whole, are positive about technologies that help improve safety. (Figure 2 and 3).

Figure 2: Bodycams, biometrics, and security cameras are considered to be positive. Most respondents have not yet formed an opinion about drones.

How do you feel about the following technologies that may be used to improve your safety?

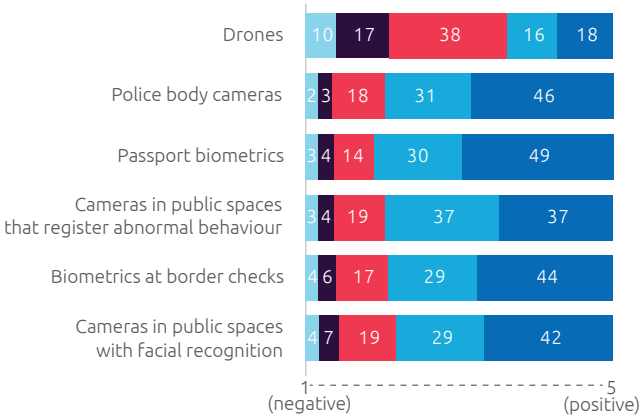
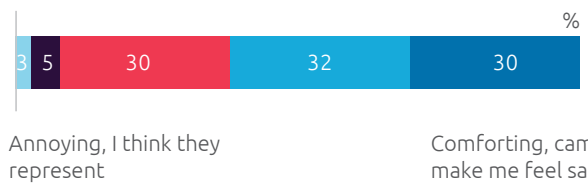


Figure 3: Cameras in public spaces are mostly regarded as comforting and safe, rather than annoying and as an invasion of privacy.

I feel the growing number of cameras in public spaces is…

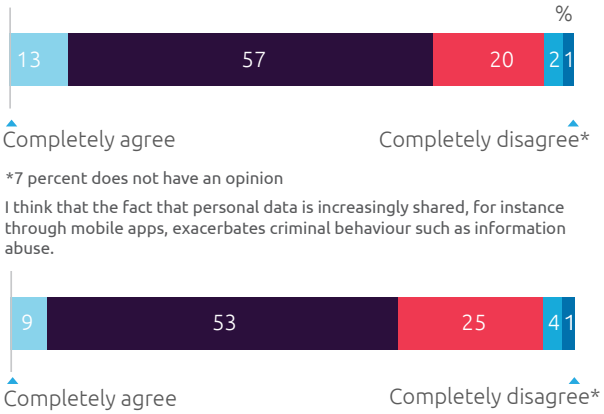


By connecting and analyzing real time data, it is (with regards to public order and enforcement) possible to predict when a shopping street will get busy or when a demonstration will start to get out of hand. This allows for timely preventive measures.

The success of the Internet of Things (or IoSTT) depends on the security of its parts, i.e. the devices. These devices are simple computers with processors, memory, software, and networking ability. This entails new vulnerabilities such as insufficient identity control, imperfect authorization, device registration issues, lack of a safe updating mechanism, and reliance upon standard passwords. Citizens are aware of these vulnerabilities. The majority of citizens feel that the level of knowledge surrounding this area should be improved (Figure 4).

Figure 4: More than 60% feel it is necessary to improve citizens' knowledge about privacy as a factor in app interaction.

To what extent do you agree with the following statements?



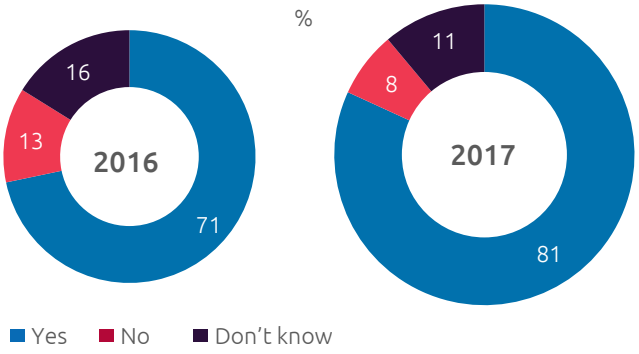
As an effective measure towards better security, Identity and Access Management (IAM) principles and techniques should be applied to these devices.

On social media, the number of threats and announcements of assaults is increasing rapidly. A murderer, for instance, recently posted a live movie of the actual murder on Facebook, including footage of him promising to make more victims. It took about two hours for the message to be removed. The larger part of threats, however, is not serious enough to warrant extra investigation. Dealing with false information on social media takes a great deal of police capacity. For this reason, the ability to quickly and thoroughly analyze social media messaging is crucial. There is enough support, among the public, for the use of social media data in the tracking down and preventing of crim inal activities (Figure 5). Plus, there is a strong conviction that the growing amount of information on social media increases the effectiveness of police work (Figure 6).

Figure 5: The absolute majority thinks that the government should make more use of social media in tracking criminal activities

Figure 6: Eight out of ten Dutch citizens are convinced that the increasing availability of information will lead to better chances of crimes being solved

Do you think that the increasing amount of information (through internet, social media, and data file integration) will influence the chances of crime fighting?



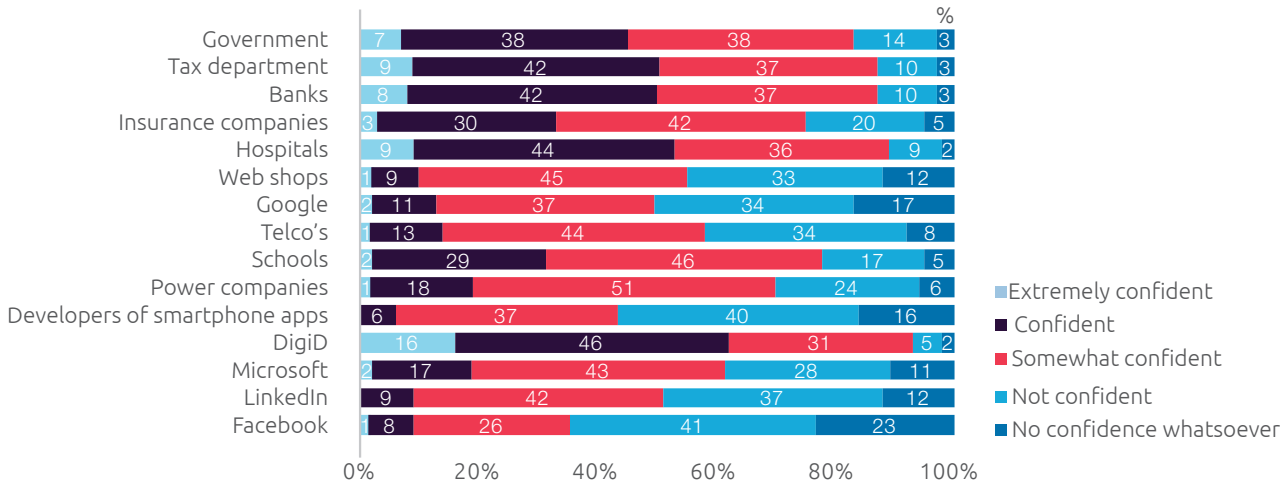
Pro-active passive monitoring allows for social media monitoring without human interference. Complex algorithms signal and analyze message contents and automatically allocate a threat level. In case of an acute or severe threat, the system provides a notification, whereupon immediate measures can be taken.

These complex algorithms are examples of a new type of artificial intelligence (AI). This type of AI is "intuitive" rather than "reasoning". In this context, "intuitive" means "making a provisional judgement based upon an observation." Such intuitions are the result of the optimization (or rather, training) of complex models through large amounts of data, until the model is able to use patterns it has learned to make useful predictions about new cases.

Incidentally, the use of Big Data analysis can also lead to better service provision. As an example, the Dutch Belastingdienst (tax department) uses different data sources to build risk profiles of citizens and companies. As such, the available capacity for enforcement can be put to use very effectively.

Figure 7: 45% of the Dutch citizens feel confident that the government handles personal data safely

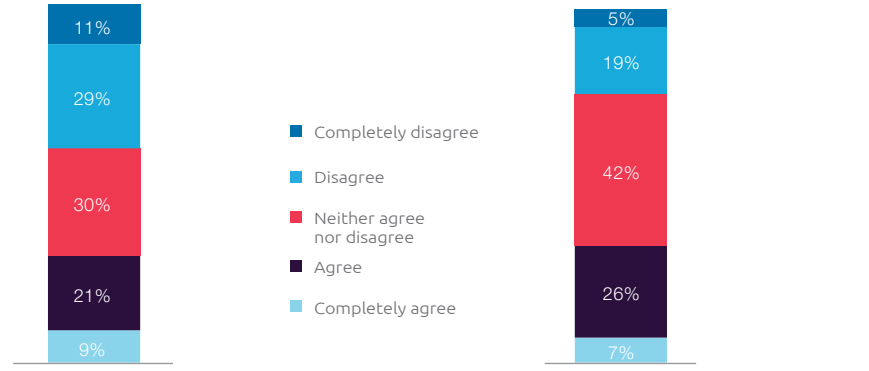
How confident are you that the following institutions will handle your data safely?



This allows for high-quality, fast and efficient service provision to the majority of taxable people; and better enforcement based upon effective case selection.

The drawback of all these new applications of technology revolves around possible infringements upon privacy. It is interesting to note that almost half of the Dutch people are confident that the government will treat data safely (Figure 7). When all household appliances start sharing and analyzing data, an accurate picture will emerge of the daily practices of the people in the household. And when smart cameras in public spaces are able to capture your movements, recognize your face, and even interpret your emotions, what are the chances of being mistakenly regarded as a malcontent, criminal or terrorist? 71% of the Dutch people are positive about the use of facial recognition cameras if this improves their safety. Luckily, the new General Data Protection Regulation (GDPR) prescribes that the development of new technologies and services should adhere to the "privacy by design" principle. As the name implies, this revolves around the direct incorporation of safety and security measures (both technical and organizational) for the privacy of individuals into the development of a new system or service.

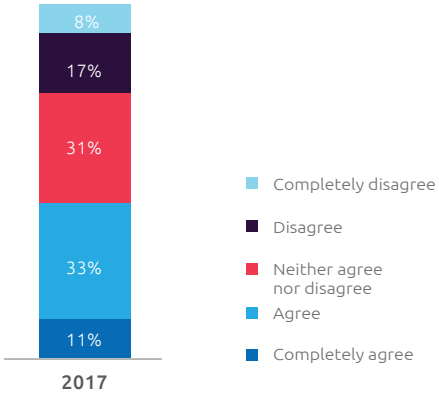
Figure 8: Four-tenths of the Dutch people are not worried about the government's increasing tendency towards privacy-sensitive measures. Three-tenths do find this development worrying.



The increase in privacy sensitive measures (e.g. facial recognition, finger print scan, and data file integration) is a cause for worry.

Civil rights are too easily set aside by the government, to the detriment of safety and security.

Figure 9: With regards to data exchange by institutions as a means to protect citizens' safety, four in ten value this goal more than their privacy.



Connections between devices, systems, and organizations result in digital networks and dependencies. According to the Cyber Security Council, however, companies hardly take into consideration the fact that, whether developing or supplying products or services, they are part of a digital chain. Vulnerabilities in one of the chain's segments will result in risks for all the others. If the Netherlands is to realise its ambition to become the "Digital Gateway of Europe," it should work to reinforce its cybersecurity at a network level. Two initiatives show that public-private collaboration can yield results: FERM in the Rotterdam harbour and the Cyber Synergy Schiphol Ecosystem. More than 40% of the Dutch people are positive about allowing data exchanging as a means to improve safety (Figure 9).

Figuur 10: To what extent do you think it is plausible that foreign powers are influencing the Dutch government?

Figuur 11: The government currently has enough means and people at its disposal to guarantee digital safety and security in the Netherlands.

If the Dutch society wants to become more digitally resilient, the Ministry of Defense may have to play a larger role than has been the case thus far. In the end, our digital society is completely interconnected with the world outside of the Netherlands. More than 70% of citizens think it is probable that foreign powers are influencing the Dutch government (Figure 10). Governmental and non-governmental actors are constantly conducting digital operations, and it is hard to distinguish between allies and enemies in the field. When we compare Dutch investments in cyber defense to similar investments of foreign countries, the term "digital pacifism" springs to mind. Meanwhile, the level of digitization of our society represents a strong argument in favor of a military strategic cyber capacity that can muster both defensive strength and offensive strike capability. Almost 50% of the Dutch people share this opinion. A majority thinks that current means are insufficient. Military defense is seen as the primary potential victim of a cyber-attack (Figure 12).

Figure 12: Almost half of the Dutch people feel that military defence and the army should be supported by the government in building cyber defences.

Welke van onderstaande organisatie(s) zou de overheid moeten ondersteunen tegen een cyberaanval?

Police (39%)	Important Dutch industries (7%)	Rotterdam harbor (9%)	Ministries (23%)	Military Defence and the army (48%)
Electricity plants (33%)	Borssele nuclear power station(34%)	Tax department (34%)	Schiphol (32%)	Waterworks (18%)
Data centres (17%)	Telephone exchanges (13%)	Banks and insurers (22%)	Social Security office (7%)	Pension funds (9%)
Health insurers (8%)	National Railway System and bus companies (4%)	Radio and TV networks (7%)	Social Security (3%)	Webshops (3%)
Credit card companies (10%)	Sensitive data of political parties	Sensitive data of charities and companies (6%)	Universities and higher vocational education (36%)	Drinking water providers (20%)

0-10%	10-20%	20-30%	30-40%	40-50%

The technological changes we have described also result in changing working methods in the safety and security domain. Changes, for instance, in the way the sector collaborates with citizens, customers, partners, and executives. This demands "agility" from organizations. This agility, however, is often thwarted by bureaucratic systems and procedures. The amount of bureaucratic systems is actually growing, further exacerbating the already significant complexity. Moreover, dealing with the cause of problems is always difficult. The fact that an alternative is possible is proven by the police organization, which has adopted new organizing principles. Principles that redirect focus towards the intention and away from the system world: back to a world where trust, quality, time, attention, and freedom of choice are paramount.

The application of these principles drives success. The example of ZSM proves as much. Within ZSM (As Fast, Smart, Selective, Simple, Collaborative, and Society-focused as Possible), Police, Public Prosecution Service, Council for Child Protection, Victim Support, and three rehabilitation organizations work together to fight common crime. In learning labs, experiments have been conducted that are aligned to the intention, whilst being in constant contact with the real environment by entering into dialogues about the wishes, needs, and chosen interventions. Along the way, it was concluded that effect measuring can make an important contribution to continuous improvement of the working process. A structural awareness of the effect of actions can help to keep the principle of working aligned to the intention, and prevent a (renewed) submergence in bureaucratic systems.

Meaningful contact between organizations in the safety and security domain and the citizen can also be promoted through the automation of simple communication. A chatbot (digital intelligence), for instance, can provide an answer to standard questions or perform referrals without the interference of human co-workers. Existing applications such as Siri, Google Now, and Cortana are good examples. In general, these bots become smarter with increased usage. To complement this advantage, the available manpower can be deployed to deal with more complicated questions, thereby improving the service level.

Contact between citizen and police often starts at the intake process. During the intake, information from different channels is processed and used as input for follow-up processes. In order to improve the connection between police and citizen in a digital society, the current communication model needs to be further expanded; and the police gearing to leverage the online possibilities even more. This requires professionalization of the service provision, by implementing an omnichannel intake organization. Omnichannel means that citizens may use any mix of different channels (telephone, website, police station, WhatsApp, etc.), but receive unified information and a unified experience throughout these channels. The channels form a seamless whole, offering a transparent process that is completely citizen-focused.

We may conclude that technological developments enable new connections, for instance: opportunities for preventive measures in the public space; opportunities to provide better services to citizens; opportunities to deploy available co-workers more efficiently. If we want to reap these benefits, we will need agile organizations that focus on the intention of their activities. This will take them away from bureaucracy and propel them to a world where trust, quality, attention, and freedom of choice are paramount.

About the author

Drs. Eric Hoorweg, MCM, is Vice President at Capgemini Consulting and responsible for the Public Order and Safety sector.

For more information, please contact the author:
eric.hoorweg@capgemini.com

Internet of Safety and Security Things. Man versus machine?

What does the Internet of Things mean for the balance between man and machine?

Highlights

- Internet of Things (IoT) is applied more frequently in safety and security solutions
- Blockchain technology offers possibility to secure IoT solutions
- Big Data analytics and Artificial Intelligence enable auto-detect and response
- Machines are catching up on humans
- However, the expert's role is not yet played out

Internet of Things makes it possible to automatically detect, analyze, assess and link events to the correct digital response scenario. Yet, the role of the professional stays crucial.

The trend of the Internet of Things (IoT) shows that more devices are connected and sensors are being deployed to signal safety and security related issues, threats and incidents. Incidents, such as explosions, accidents, terror attacks and cyber-attacks, or the threat of it.

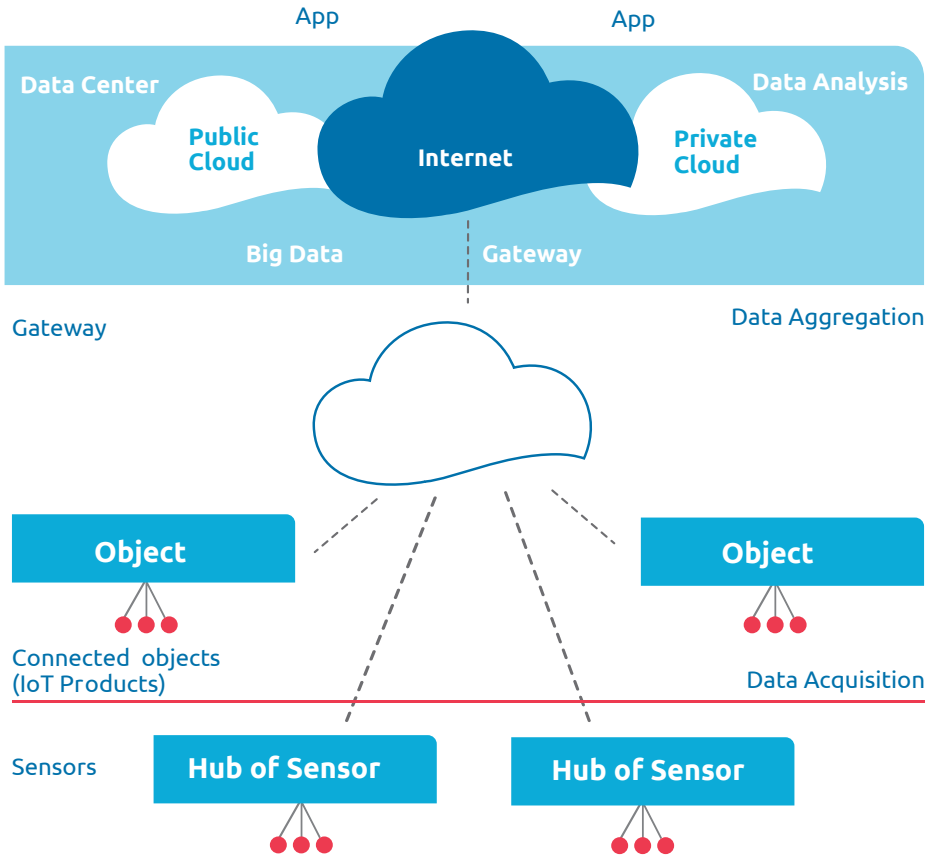
Internet of Safety and Security Things (OSST) can combine and analyze detected signals from the sensor network, and is then able to determine that a safety or security event is occurring. Because of the connection to the IOSST to Safety and Security Incident Response Management System (SSIRMS) an adequate and fast response can by automated. Does this mean that the human factor to respond to a wide variety of security issues disappears? And does this make our society safer? The March 2017 Kantar TNS research indicates that almost half of all citizens are concerned about humans losing grip on machines.

Figure 1: Grip on Thinking Machines

Internet of Things

The Internet of Things consists of sensors connected through networks on computer systems. These systems monitor and drive connected objects and machines. The connected sensors can also monitor the real world, humans and animals.

Figure 2: Internet of Things



Source: Securing the Internet of Things Opportunity: Putting Cybersecurity at the Heart of the IoT; Capgemini Consulting & Sogeti High Tech; 2014 the IoT; Capgemini Consulting & Sogeti High Tech; 2014

IoT has different usage levels:
1. Remote reading of sensor information;
2. Controlling sensors/activators;
3. Act on sensor information based on algorithms, without the intervention of people
4. Totally new products and services that were not possible without IoT.

Meanwhile the technology is available to (fully) automatically detect, analyze, assess and link events to the correct digital response scenario. The physical response organization can use this for shared situational awareness and to evaluate post-deployment.

Internet of Things and blockchain grow towards each other
When deploying a reliable network of thousands of sensors for safety and security issues, privacy and reliability are important aspects. The decentralized, distributed character of blockchain technology offers the opportunity for sensors to reliably and robustly exchange information and transactions across chains.

The blockchain is a distributed database in which transactions are being recorded through cryptography in a way that unauthorized persons can't carry out transactions without being detected. This allows database availability for all participants without a central supervising authority to guarantee the accuracy and safety of the data. Blockchain technology is the technology that enables blockchain. The technology consists, among others, out of the database and software to create and control digital identities, to register transactions on the blockchain and to share the database with participants[1].

Although blockchain has its origin in the financial world, the technology is also very suitable for securing sensor signals and transactions. Because of this the Internet of Things solutions can assume the reliability of the signal that is being exchanged.

Acronis (supplier of cloud backup, disaster recovery and secure file share solutions), for instance, is extending its own data storage and file sync & share solutions with blockchain technology, to monitor and safeguard the integrity and validity of data. Examples of data using blockchain for security against manipulation are: property and medical files, stock transfers, judicial evidence, police videos or images of security cameras that can be subjected to IT-audits.

Internet of Things and Big Data complement each other

The sensors connected to the Internet of Things offer a variety of information and applications within safety and security. The volume of data generated through these sensors is however soon too much to process for humans. Internet of Things analytics is necessary for analyzing the huge amount of data. Research and advisory company Gartner[2] expects that the distributed network will also carry out the analytics distributed. Artificial Intelligence (AI) and self-learning systems are needed to carry out these analyses and to predict or trigger the correct response.

Automatic processing wins from the human being

AI is becoming more advanced. Sensors and AI in self-driving cars are better at assessing certain traffic situations than human beings. Because of the large number of sensors, sophisticated sensor combinations and smart algorithms for processing sensor signals, machines can react and communicate faster than a human expert. In surroundings where this velocity is needed, the role of the human expert will disappear, reduce or at least change.

The unmanned control room?

For many years the control center has been at the heart of every safety and security organization. Will this heart soon only pump digital information and solemnly consist out of IT? To answer this question, we will put this into practice. How do we react now and will we react later to a cardiac arrest when every second counts? Now we signal a colleague's (possible) heart failure and call the internal emergency number. According to protocol, the control room staff member sends for people that can assist. This can be your own company rescuer or the ambulance. After a few minutes, your colleague receives initial necessary professional help.
Later, the IOSST signals that an AED device has been pulled of the wall on the fourth floor and that within a 20-meter radius, a person's smartphone made a falling motion in a room on the same floor. The surveillance camera and motion detector connected to the IOSST automatically detect a person laying quietly on the ground. Within 1 second of the first received signal, the IOSST concludes that a person needs help and classifies it as a (possible) heart failure. The Indicative Response Management System (SSIRMS) automatically carries out the "(possible) heart failure" protocol and passes it along with the location to the company rescuer on the same floor and to the emergency control room. After a few seconds ("Every second counts") without human interference, someone receives the initial necessary professional help from a human being. In this case the company rescuer.

---

[1] https://www.nl.capgemini.com/resource-file-access/resource/pdf/3._het_gebruik_van_blockchain-technologie_in_nederland.pdf
[2] Gartner; Top 10 IoT Technologies for 2017 and 2018; 22 January 2016.

So the IOSST clearly takes the lead when it comes to quick observation, first assessment and response. Humans still stand at the top for the second assessment, managing the situation and providing expert assistance. This role distribution between IT, people and professionals is embedded in SSIRMS's tested and practiced protocol. The software will soon win when it comes to combining and reviewing various initial data and the speed of action. The role of humans has indeed disappeared or at the least changed in the IOSST, but is still crucial.

The previous scenario is an example that can be fully achieved today with the current state of technology. Therefore "later" may already be in a few days.

Our conviction is that the expert's role has not yet been played out. The digital transformation that will cause Internet or Things will change the role of the expert. It will be an interesting learning curve between people and machines to determine how to complement each other.

The human factor is still important in safety and security issues. It is necessary to continue to work on risk awareness, to make the right estimation of potential risks and create a solid crisis communication and an incident management system, in order to properly coordinate crises response. The role of man has indeed disappeared or become different in the IOSST, but is still crucial.

Many organizations with their own specific safety, security and cybersecurity issues can gain from Internet or Safety and Security Things when it comes to combining and reviewing various data and speed of action, whether or not in combination with an Indicative Response Management System.

About the authors

Erik van den Berg MSc is a principal consultant at Capgemini. Paul Lengkeek MSc is a managing consultant at Capgemini. They are specialized in developing and implementing information systems in the crisis management domain.

For more information please contact the authors:
erik.e.vandenberg@capgemini.com, www.linkedin.com /in/erikvdbergcapgemini and paul.lengkeek@capgemini.com, www.linkedin.com/paul-lengkeek-8551183

More strike fighters or more digital weapons systems?

Are we making the right choices in our defense budget spending, in view of the digital threat in the world?

Highlights

- More Dutch people are increasingly concerned about a digital attack on our country, rather than a physical attack
- Nevertheless, the armed forces continue to invest heavily in traditional weapons systems

Our prosperity and our values are deeply connected to and part of the digital domain. Our digital freedom has therefore become an essential part of our vital infrastructure. This requires robust protection measures.

This is not new. In both the public and private sector, many interventions have improved digital security successfully for years already. But after the shocking revelations concerning the influencing of the US elections, we must question whether our existing protection measures are sufficient. And whether we actually know to what extent our national private and public digital domain has been infiltrated and manipulated? And by whom?

So, we need to discuss the sufficiency of our national digital protection, given the scale and scope of international digital operations. Snowden and Wiki Leaks publications have already given us a first insight in US digital power. From many observations[1], it is concluded similar impressive digital capabilities have also been developed by other major powers. Both by our traditional allies[2] and other world or regional powers. In the digital domain, however the distinction between ally and enemy is not exactly clear. Important allies have no scruples about infiltrating[3] their friends, as evidenced by Belgacom's hackers and the tapping of Merkel's phone. And this is nothing new in world of espionage. It is vitally important to check your ally's loyalty continuously.

We do not choose the future battlefield ourselves. Today, the international arena is no longer in the Northern part of Germany, in the desert or on the open ocean. The battle arena of our enemy is in the connected network through which we share information and carry out transactions. The world powers capabilities to carry out infiltrations and manipulations in the digital domain is impressive. But how can a small- or medium sized peace loving sovereign country then protect itself effectively? For them appropriate capabilities are hard to realize. Is there a role to play for NATO or the EU?

The NATO alliance traditionally focuses on physical territorial security, protected in a traditional and analogue way. Although in NATO cybersecurity threats and measures are widely published and discussed, there is no real operational capacity available. The NATO Cooperative Institute for Cybersecurity in Tallinn is a good example of this. This is a Center of Excellence, not a headquarters. NATO focuses on knowledge building and knowledge sharing and is limited to cyber defense against traditional enemies. Defense against your own allies is, of course, not on the agenda.

Currently efforts are being made to develop cyber capacities within many medium-sized NATO member states[4] bilaterally. NATO's main players run vast digital capabilities and are understandably reluctant to share this knowledge widely. Cyber capacities are highly strategic and comprise a strong intelligence component. And finally, as NATO is a defense organization exclusively and important decisions are taken unanimously it is practically impossible to build a capability that might have an offensive element. All in all, it can be said that NATO plays virtually no role in the most important and current domain of international security at this time.

What about the EU? The EU is also aware of its digital single market[5] cyber vulnerability as highlighted in the 2013 EU Cyber Strategy report. The EU Parliament itself also has independently conducted various investigations but this has, so far, not led to any cyber capacities. Furthermore, it is clear that the EU, despite increased collaboration under the Directive on Security of Network and Information Systems (NIS Directive), has neither the infrastructure nor the mandate to play an effective role on the world's cyber stage.

The major powers in the East and West have powerful digital infiltration and manipulation capabilities deployable for own national interests. NATO or the EU cannot provide a protection or support umbrella for the Netherlands in the digital domain.

For effective protection against foreign cyber operations the Netherlands can therefor only rely on itself. What is the Netherlands actually doing for this right now?

In the Netherlands, we have a Defense Cyber Command (DCC) since 2013, with about eighty specialists, according to the latest public data[6]. DCC's main task is to support analogue military operations. Protecting Dutch digital society against foreign secret services is explicitly no responsibility for the Defense Cyber Command.

The civil National Cyber Security Center (NCSC) is only an "information and expertise center". The NCSC has no operational capacity or intervention mandate. It has no role in providing protection against foreign secret services.

---

[1] http://www.cfr.org/china/mandiant-apt1-exposing-one-chinas-cyberespionage-units/p30020

[2] http://www.volkskrant.nl/tech/wat-ziet-de-vlieg-op-de-muur-allemaaldit-weten-we-nu-over-de-nsa-spionage~a3530819/

[3] http://www.spiegel.de/international/europe/british-spy-agency-gchqhacked-belgian-telecoms-firm-a-923406.html

[4] http://www.NAVOlibguides.info/cybersecurity

[5] http://www.europeanpublicaffairs.eu/time-to-catch-up-the-eus-cybersecurity-strategy/

Since 2014, the Military and the Civil national intelligence agencies have been working together to bundle their cyber activities in the Joint Sigint Cyber Unit (JSCU). This unit will eventually comprise 350 staff members. However, collaboration between these two competing national intelligence agencies, each with its own closed corporate culture, is not easy[7]. Both groups work with their own systems, their own resources and their own goals. It is therefore uncertain what this collaboration will produce. From their own publications, it appears that a substantial part of their resources is related to Jihadist network[8] research currently. The question is how much time is left for the real international "advanced high-tech cyber domain"? Webservers on a distant small polder city[9] in the Netherlands were part of the network used to influence the American elections. It is painful to observe that our country is obviously recognized as a safe haven for this kind of operations.

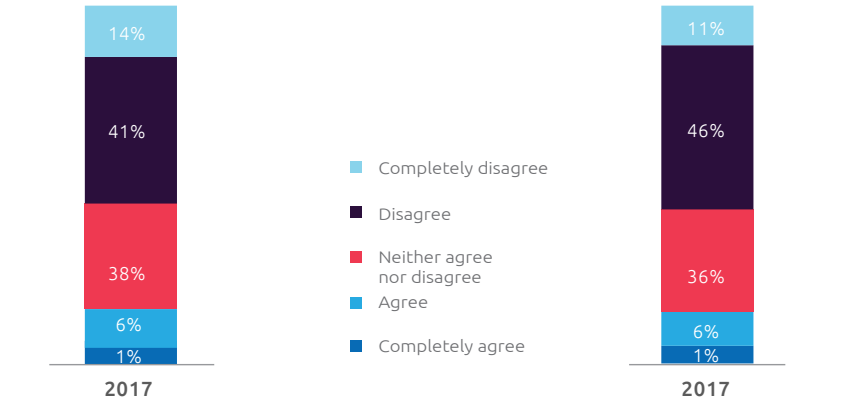
The "cyber task" of our national Joint Sigint Cyber Unit is gathering information through cyber operations, as well as investigating and preventing threats, attacks and espionage against Dutch computer networks. However, offensive cyber operations are legally exclusively mandated to the Defense Cyber Command (DCC), with a staff of approximately 80 people.

The Personal Data Authority (AP in Dutch[10]), formerly known as the College for the Protection of Personal Data, will make an important contribution to improving digital security in the Netherlands by enforcing the Data Protection Act/General Data Protection Regulation. And with that, the AP will contribute to the protection of our privacy; one of the essential values of Western society. However, in the context of international cyber operations, the AP hardly plays a role, since it does not have its own tracing or detection capability.

Only 7% of survey respondents consider that the Dutch government and companies are sufficiently prepared for a possible cyber war.

[6]https://nl.wikipedia.org/wiki/Defensie_Cyber_Commando
[7]http://www.telegraaf.nl/binnenland/22340487/__Spionnen_onder_een_dak__ruzie__.html
[8]https://www.aivd.nl/actueel/nieuws/2016/03/31/koning-opwerkbezoek-bij-joint-sigint-cyber-unit
[9]http://buitenland.eenvandaag.nl/tv-items/69575/nederland_spil_in_russische_hackcampagne_tegen_vs
[10]https://autoriteitpersoonsgegevens.nl/
[11]http://www.cfr.org/china/mandiant-apt1-exposing-one-chinas-cyberespionage-units/p30020

Figure 1: Only 7% of those surveyed consider that the Dutch government and companies are sufficiently prepared for a possible cyber war.



The Dutch **government** is sufficiently prepared for a possible cyber war.

Dutch **companies** are sufficiently prepared for a possible cyber war.

How is Dutch digital society protected?

This article started with the question who is protecting our national values in this digital age and to what extent are they succeeding? We find that many organizations are working in the various sub-sectors of cyber security. But the question remains: who is currently working on protecting our national digital values and infrastructure against the advanced capabilities of the global powers?

The only entity in the Netherlands that has the mandate and resources to carry out this task is the JSCU with its 350, or so, employees. But we also note that real cooperation within this alliance appears difficult. If you discount this group's non-productive bureaucracy and assume that a substantial portion of its efforts are concerned with Jihadism, this leaves only a relatively small portion to monitor the activities of the NSA and its equivalents in other Western and non-Western major powers.

The Military and the Civil national intelligence agencies have a combined budget of around € 300 million available to them for roughly 2,000 employees according to public sources. The JSCU will logically not have an annual budget exceeding € 60 million.

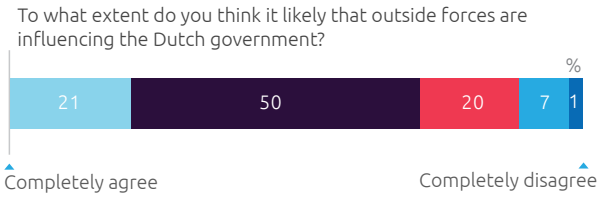
To fill in the picture: the NSA alone has 30,000 employees and a budget of US$ 10 billion. In addition, the many other security services in the US, such as the CIA, FBI and the Ministry of Defense, also have their own substantial cyber divisions. On top of this, inside the military each of the military forces have their own separate and substantial cyber capacity. And undoubtedly many other services (Homeland Security, Coastguard, Customs, DEA, etc.) have their own cyber units too. Unless and until a Chinese or Russian Snowden comes forward, we will know little about the cyber capacities of the other major powers. But it appears from many publications[11] that the capacities of China, Russia, the UK and France are also considerable. And there is no reason to doubt that countries such as Turkey, Iran, Indonesia, Japan and India also have substantial cyber capacities.

What should the Netherlands do?

The digital arms race started a long time ago already. A digital pacifist standpoint could be that you reject the immorality of these capabilities and hope that others respect this honorable standpoint. But if you think that our prosperity and values are deeply connected to – and part of – the digital domain, you must also provide adequate protection. Protection that is at least proportional to our economic and strategic position in the world and of such a range and quality that others will think twice before trying to infiltrate and harm the sovereignty of our national digital domain.

Our historic alliance with the US is changing due to globalization, new American leadership and international terrorism. The impact of massive army divisions, squadrons of fighter planes, aircraft carriers and submarines has also changed. National security (homeland security) is the domain of special forces, covert operations, drones and robotics. These can only be applied effectively using wide-ranging and advanced digital resources. These digital resources are being applied everywhere and, in doing so, the US is not restrained by territorial agreements with allies. As long as this is not detected or prevented, these resources may also be operated against our own country.

Figure 2: More than 70% of Dutch people consider it likely to very likely that outside forces are influencing the government.

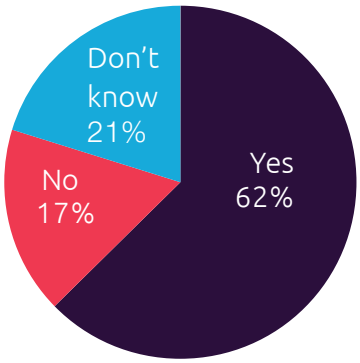


The Netherlands' GDP amounts to roughly 5% of American GDP. If we use the US as a benchmark, the Dutch equivalent to the NSA would employ 1,500 people and have a budget of € 500 million. Since we have a large shortfall to make up and the rest of the world is a much bigger place for us than for America, it would actually be reasonable to expect these figures to be much higher.

The Dutch armed forces have a budget of approximately € 8 billion per year. Alongside personnel costs, the largest portion of the budget is spent on the acquisition and maintenance of very expensive, traditional weapons systems. The portion spent on digital warfare is negligible. This is noteworthy when you consider that the chance of a digital attack on the Netherlands is by many considered to be much more likely than the chance of a physical attack.

Figure 3: More than 60 % of Dutch people consider the chance of a digital attack on the Netherlands more likely than a physical attack.

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



What would the Dutch NSA do with that budget?

What the Dutch NSA actually needs to do in the cyber field is to practice the Clausewitzian "Art of War" in a digital manner. This type of warfare has nothing to do with acquiring and building up large stocks of weapons. Clausewitz's art is in the creative application of the available resources and the mobilization of the will to win the war. This begins in academies and institutes where the best strategists together study how to achieve desired effects and develop scenarios for the digital battlefield. The most likely scenarios then form the basis for the build-up of cyber capacities. This militarily strategic cyber capacity constitutes a deterrent in itself to protect our connected society. It ensures that the "others" know that each infiltration or manipulation will be retaliated equally.

Through this protection, we not only improve our own security but moreover we can invest safely in new digital innovations in the private and public sectors. And when we have done that we also could consider starting vote digitally, without any concerns.

About the authors

Erik Hoorweg MCM MSc is vice president at Capgemini Consulting and responsible for the public order and security sector. Peter Kwant (Executive Master Security & Defense) is a principal cyber security consultant at Capgemini and former naval officer.

For more information please contact the authors:
erik.hoorweg@capgemini.com, www.linkedin.com/in/erik-hoorweg-296b593, @ehoorweg and peter.kwant@capgemini.com, www.linkedin.com/in/peter-kwant-06b5b811

Computers with intuition: get used to it!

In what way are new artificial intelligence applications different from the old ones? And what does this mean for the tasks for which they can be deployed?

Highlights

- Intelligence comprises two cognitive functions: logical reasoning but also the ability to make a good preliminary assessment based on perception (intuition)
- The new wave of AI applications is making enormous strides in terms of the intuitive aspect
- It is possible to apply these new AI techniques to entirely new areas, especially where explicit rules are not applied
- Government and society need to get used to intuition-based computer applications

The new wave of artificial intelligence (AI) applications approaches intelligence in a different way than in the past: the applications are more "intuitive" than "reasoning" in character. This certainly produces opportunities, but also risks to the ways in which those systems can be deployed in society.

You might not think about it every day, but our brains actually know two tricks, also called cognitive functions: Type 1 is fast and predominantly associative and intuitive; Type 2 is slow and more reasoning. For example, if you are driving a car and approach an unclear situation at an unfamiliar intersection, the Type 1 processes in your brain cause you to ease off the gas and reduce speed in good time without really being conscious of it. Afterwards, you evaluate the situation, taking into consideration the other vehicles, traffic signs and traffic rules that tell you whether you have priority or have to stop. The latter is typically a Type 2 process. An interesting question here is what we are talking about when we speak of artificial intelligence in computer systems. Do these systems simulate Type 1 or Type 2 processes? And what does this mean for the position they are able to assume in a connected society?

The first serious steps in the field of AI were taken in the 1990s: can we simulate brain functions in the computer? At that time, development focused primarily on Type 2 thinking: creating a reasoning super brain. The unspoken belief at the time was that, in terms of intuition, man would maintain control over the computer, at least for the time being. Unfortunately, the practical applicability of these reasoning systems, at the time, lagged behind the perhaps somewhat overestimated expectations, although applications like chess computers, TomTom routers and business rule-driven systems can be considered useful products resulting from this development.

At present, a second and much larger wave of AI applications is on its way. Remarkably, it is in Type 1 thinking that computers are suddenly making great strides. This is due to a confluence of three developments:

1. The huge amounts of big data available to train these systems (in which the increasing availability of open data is also an important factor);
2. Advances in the necessary underlying algorithms and mathematics;
3. (mainly) The development of available memory capacity and computing power.

The latter is possible through processes that were originally developed for graphics cards (GPUs), making computers better and faster at advanced predictive analytics. This is not achieved through calculation and reasoning, but by using complex models to optimize (train) computers to process these large amounts of data until the model is capable of making meaningful predictions about new cases, based on previously observed patterns.

The computer may be ready, but is mankind? We are used to computers beating us at chess, but a computer that performs better than someone with years of experience in assessing files for potential fraud, detecting cybercrime or predicting the outcome of a lawsuit based only on a case file; that is something to which we are not yet accustomed. Without noticing, we already use these types of system every day. Examples include the Google, Facebook and Netflix algorithms that determine which hits, posts, movies and ads we receive. Virtual assistants, like Siri, Google Now and Cortana, are also getting smarter every year. The same goes for computer translations, like Google Translate, that are currently becoming context aware in many languages by applying neural machine translation (NMT). In many cases, these translations can no longer be distinguished from a human translation. Computers can already perform lip reading better than most people. Perhaps most worryingly, computers are as good as people at completing anti-robot filter puzzles, like CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart). Computers have also already defeated human beings in other direct confrontations, such as Jeopardy (IBM Watson) and recently also Go (Google Deepmind). The latter's goal is now to defeat human opponents in the real-time strategic computer game Starcraft II.

Computers are also developing on a creative level. Neural networks can transform photos into paintings in the style of different artists. Last Christmas, Capgemini Norway, in collaboration with Microsoft, had a computer compose a Christmas song by training it for two weeks on 50 existing Christmas songs.

In this specific challenge, human songs still turned out to be better than computer songs, but for how long?

For society as a whole, especially in the domains of public order and security, huge opportunities and challenges exist. Opportunities because this is still relatively unknown territory, in which many wonderful applications are undoubtedly hiding. The new AI systems can best be used on applications for which no exhaustive explicit rules can be formulated, but for which a great deal of experience data is available. Challenges because both government and citizens are not yet used to the idea and we do not yet know all the pitfalls. How "clever" do citizens want a system to be before the situation becomes uncomfortable and is seen as a threat to privacy? What data may we actually use and how does the system react when data is "polluted"? Can unwanted effects like ethnic profiling be adopted by your knowledge system through its training on historical data? How does a judge explain to a convicted person why they are also being given community service, in addition to a fine, because the system estimates a high risk of recidivism? And that the computational model is so complex that we cannot really retrace how the system has arrived at that risk assessment? This may be the biggest danger with these Type 1 systems: they are and remain automated intuition. As humans, we want to translate things into reason, logic and then discuss them. Perhaps this is something for the next generation of AI?

About the author:

Frank Inklaar is a senior consultant at Capgemini. He focuses on applying advanced analytics and artificial intelligence in the field of public order and security.

For more information, please contact the author:
frank.inklaar@capgemini.com and www.linked.com/in/frankinklaar

More anonymous by deploying new technology? Privacy by design makes it possible!

In what way does “privacy by design” increase the careful use and acceptance of new technologies, such as automatic face recognition?

Highlights

- New technologies, such as automatic face recognition, offer increased opportunities for monitoring
- Privacy by design is a way for the government to deploy potentially invasive technologies carefully and effectively
- Privacy by design, often still a container concept, must be defined over the coming period
- The government can set the right example and be transparent about the measures taken
- The government can stimulate the sharing of best practices

More and more organizations in the public safety domain are putting new technological capabilities, such as automatic face recognition using smart cameras, in place to improve monitoring. Many of these technologies invade the personal privacy of individuals. Applying “privacy by design” prevents the negligent use of potentially invasive technologies.

Following the attack at the Christmas market in Berlin last year, people in Germany immediately asked whether the perpetrator could have been arrested earlier if more surveillance cameras had been placed in public spaces. In a country in which personal freedom and privacy are very important, public opinion shifted: in the fight against terror, people seemed more willing to give up some of their anonymity. New technologies are offering increasing opportunities for supervision. Although some technologies are still under development and in testing, new cameras are already able to track people on the street and to identify and recognize facial emotions. No more moving around anonymously in public spaces: for some a frightening prospect befitting a police state, for others a necessity to keep modern society safe.

Acceptance of privacy-invasive technologies in public spaces depends to a large extent on the purpose for which the government applies a particular technology. Research from Kantar TNS, for example, shows that 71% of the Dutch population is positive about the use of face recognition cameras, as they increase their safety. On the other hand, only 43% of the Dutch population trusts the government to adequately protect their privacy. There is room for improvement in this respect, therefore.

Figure 1: What do you think of cameras (possibly) being used to increase your security?

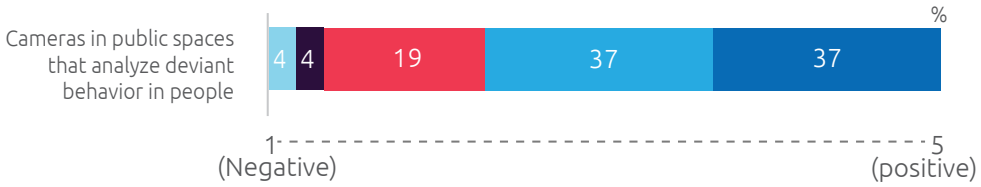
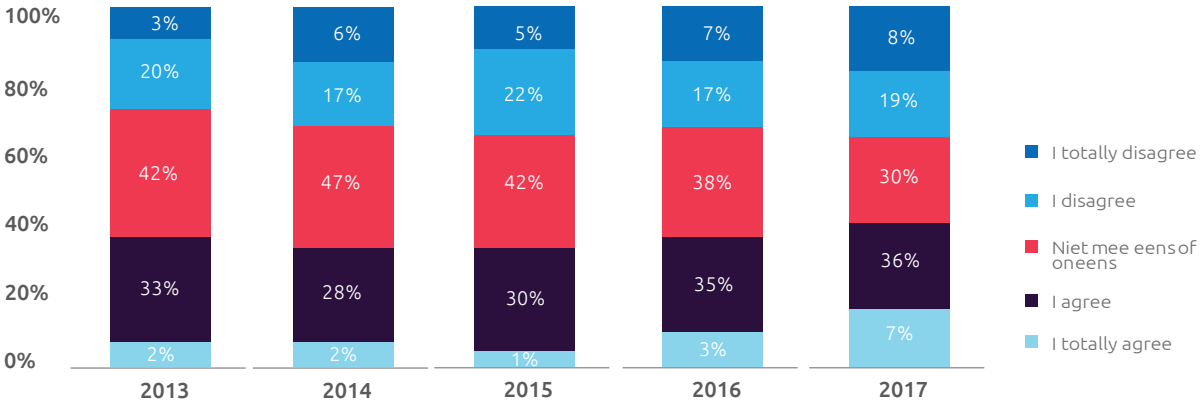


Figure 2: The population is divided in its trust of the government's privacy protection

I am confident that the government protects my privacy adequately



Privacy by design is a way for the government to deploy potentially invasive technologies carefully and effectively, to be transparent and, at the same time, not to unnecessarily invade the privacy of citizens. It is important, however, for privacy by design, often still a container concept, to be defined over the coming period. The government can play a role in this by setting a good example and encouraging the sharing of best practices.

Automatic face and emotion recognition

The technology for recognizing faces automatically has recently improved significantly. Automatic face recognition means the automatic processing of digital images containing individuals' faces for the purpose of identifying, verifying, or categorizing those individuals[1]. In its report published in 2015, "Close to the skin: emotion and face recognition in the Netherlands", the Rathenau Institute names five types of application in which the face is used as an information source: verifying, identifying, matching, categorizing, and emotion recognition[2]. The Rathenau Institute describes the five applications as follows:

- Verifying: Checking if a person is who they claim to be. The face is compared to a previously saved template or image of their own face.
- Identifying: Comparing a live image of a person with images or templates in a database. The face is compared to the entire database.
- Matching: Comparing images in a database instead of a live image with a database. The goal of matching is to match images of the same person.
- Categorizing: Categorization is aimed at extracting information that is not directly linked to a single person, such as group attributes like age, race, and sex.
- Emotion recognition: Translating facial expressions or other characteristics of a person into their emotion or general state of mind.

[1] Article 29 data protection working party 2012, p. 2

[2] Dicht op de huid: gezicht- en emotieherkenning in Nederland, Rathenau Instituut, 2015, p. 11

Face recognition privacy impact

The impact on an individual's privacy differs per application, but certainly depends on the purpose for which – and the context in which – it is deployed. The impact of verifying, identifying and matching images may be smaller when the individual is previously informed and in a context in which it is expected (for example, at airport customs) than when it happens unnoticed at a location where anonymity is expected. Categorization can be very sensitive because characteristics such as race, age, and gender reveal a lot of information about our identity. When it is impossible to trace information back to an individual (for example, when it is only possible to verify that the person in question is a man), the impact is naturally less or non-existent. With emotion recognition, the impact is particularly high when a person thinks they are anonymous and are unaware of their facial expression. Also, new technical developments, such as linking databases more easily, may have a greater impact on individuals' privacy. What exact impact a particular technology and application has on privacy is therefore difficult to determine, in general.

Applications of face and emotion recognition in the security domain

Camera surveillance using automatic face recognition is nothing new. Organizers of major (inter) national events, such as the Olympic Games, the soccer World Cup, the US Super Bowl and national soccer matches already widely apply the technology. Airports have also been experimenting with guiding passengers through customs faster. For example, Schiphol Airport, following on from the airport in Aruba, has been carrying out automatic face recognition tests to guide passengers through customs faster. Passengers only have to show their passport once in the terminal. By means of face recognition, the passenger can then check in, hand in luggage, cross the customs border and board the plane without having to show a passport or boarding pass again. In this instance, a match is made between the live image and the photo on the passport. Automatic face recognition is also applied to countless local initiatives. In Rotterdam, where certain people are banned from public transport, tram lines apply the technology. In the US, local police teams apply the technology to take a photo during an arrest and store it in a database. In its Next Generation Identification (NGI) program, the FBI is considering the possibility of expanding face recognition and linking various databases for national security reasons. When this development is expanded internationally, it will inevitably lead to privacy discussions.

Privacy by design

Privacy has gained greater attention in recent years, due to the emergence of new technologies. Legislators respond to this by drawing up legislation that better protects the rights of individuals. New European Legislation, the General Data Protection Regulation (GDPR), states that when developing new technologies and services, "privacy by design" (or "data protection by design") should be applied.

At the very least, privacy by design consists of the following elements:

- Include protection of the privacy of individuals whose personal data is being processed directly in the design of a system or service
- Take appropriate technical measures to control access to and usage of personal data and enable it to take place securely.
- Take appropriate organizational measures to control access to and usage of personal data in accordance with certain agreements and regulations.

Organizations responsible for processing personal data should consider appropriate technical and organizational measures per application, to protect the privacy of individuals. Technical measures relate to information security, ensuring the availability, exclusivity and integrity of all forms of information within an organization. An example of privacy requirements for which technical measures must be taken is: the requirement that only proper and authorized persons may gain access to certain information for a clearly defined purpose. To do this, systems must be properly configured. Other examples are that data may only be stored for a certain time, that it should be properly destroyed, and that an individual should be able to exercise control over his/her data in an effective way. This should be considered when designing a system. Organizational measures include, for example, raising awareness in people who work with (sensitive) personal data, transparency towards the people whose personal data are processed and clear communication.

When privacy is included directly in the design of applications, it can work as an enabler in using the correct applications for the correct pre-determined goals. This prevents applications being introduced negligently, in hindsight, and therefore gaining little support in society.

Role of the government

The government can play a crucial role in creating support for new technologies. For example, the government can develop a balancing framework for organizations that use new technologies. The framework can provide a careful balance between the goal of a new resource and the invasion of citizens' privacy. The government can then set a good example by being transparent about this balance and the privacy enhancing measures it takes when new technologies are deployed. Finally, the government can encourage the sharing of best practices in the domain of privacy by design. Effective monitoring using modern technologies and adequate protection of individuals' privacy are not mutually exclusive. New technologies offer unprecedented possibilities, but it is important that direct attention is paid to privacy during their development. What appropriate technical and organizational privacy measures consist of differs per technology and application. Privacy by design must gain more substance over time. The dreadful picture outlined by George Orwell in 1984 that you had to live on the assumption that every sound you made was monitored and every movement studied – Big Brother is watching you – does not need to come to pass. Paradoxically enough, automatic face recognition may even ensure greater anonymity in public places because a computer and not a human being (as with security cameras) monitors the images. It is important, however, that the government is transparent about the use of new technologies and the way in which it implements privacy by design in their development.

Privacy by design implies that appropriate technical and organizational measures are taken in order to provide adequate privacy protection when determining the methods by which personal data are processed and in the actual processing of personal data. It is therefore necessary to pay direct attention to privacy when designing processes and systems.

About the authors:

Christian le Clercq LLM MSc and Bart Bikkens MSc are both senior consultants at Capgemini Consulting. They specifically focus on issues relating to privacy, national security and crisis management.

For more information, please contact the authors:
Christian.leclercq@capgemini.com, www.linkedin.com/in/christian-le-clercq-7a74239, @cleclercq and bart.bikkers@capgemini.com, www.linkedin.com/in/bartbikkers, @BartBikkers

Cybersecurity as a prerequisite for strong chains

How can chain partners together strengthen their cyber resilience?

Highlights

- Organizations become digitally dependent on each other
- Manifestations make vulnerabilities, threats and risks visible at chain level
- Hardly any insights exist into chain dependencies
- Collaboration at chain level is essential

Organizations are part of chains and are, therefore, dependent on the cyber resilience of their partners, making collaboration at chain level essential.

Digitally dependent

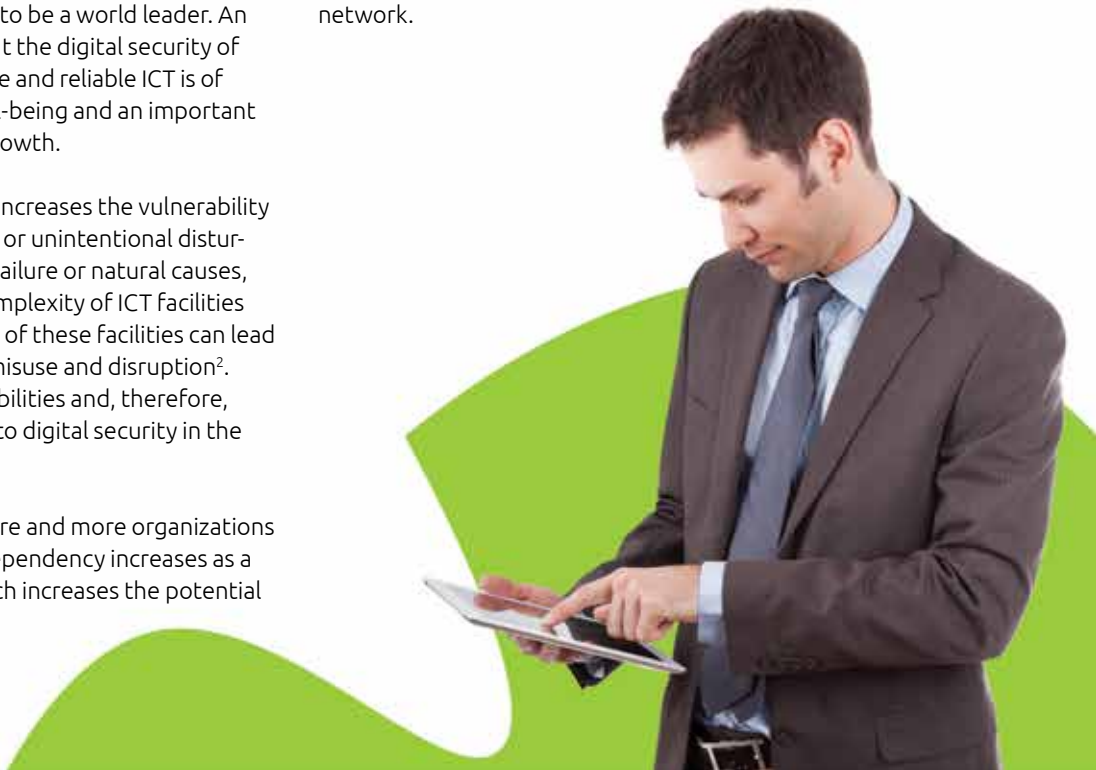
One of the Netherlands' ambitions is to become the Digital Gateway to Europe[1]. When it comes to using and deploying ICT in society, the Netherlands aims to be a world leader. An important prerequisite for this is that the digital security of the digital society is guaranteed. Safe and reliable ICT is of fundamental importance to our well-being and an important impulse for sustainable economic growth.

ICT provides opportunities but also increases the vulnerability of continuity in society. A deliberate or unintentional disturbance, due to a technical or human failure or natural causes, can lead to social disruption. The complexity of ICT facilities and the increasing interdependence of these facilities can lead to new vulnerabilities and result in misuse and disruption[2]. Cyber criminals abuse these vulnerabilities and, therefore, represent an ever-increasing threat to digital security in the Netherlands[3].

The business process systems of more and more organizations are connected to each other. This dependency increases as a result of the Internet of Things, which increases the potential impact of a disturbance in the chain: damaging the interests of one part of the chain can have consequences for the chain as a whole. A chain is only as strong as its weakest link. If the interests of one party are at stake, this will automatically affect the other parties in the chain. For this reason, individual or organizational interests become shared interests.

The risk of the weakest link

That organizations are becoming more and more dependent on each other's systems and data is nothing new. From a corporate perspective, public and private organizations increasingly go beyond their own organizational boundaries to work more effectively and efficiently. But according to the Cyber Security Council, companies and governments barely take into consideration the fact that they are part of a digital chain[4] in which they develop or deliver products and services. Common interests, dependencies, vulnerabilities and various types of cyber threat are increasing. But what does this increase mean for public and private organizations? Based on a few examples of manifestations, we can show how these dependencies impact many organizations that are linked as part of a chain or broader network.



Hack of Antwerp container company[5]
Between 2011 and 2013, the container logistics system in the port of Antwerp was hacked for the purpose of allowing illegal drug containers to pass. The criminals used different forms of cybercrime. They hacked a number of major processing companies in the port of Antwerp by using, among others, a phishing method. The hackers knew exactly where their container was located and manipulated the system so that the container was placed in a favorable place in the port. In addition, they gained access to the terminals' unique PIN codes to release the container. The Justice Department estimates that more than a ton of heroin, almost three tons of cocaine and rare minerals have been brought in this way. In this case, data protection plays an important role: the prevention of the manipulation and/or stealing of data.

DDoS on DigiD
The DDoS attacks on DigiD illustrate the impact that an attack can have on an important link in a chain. The limited availability of DigiD, due to several DDoS attacks in mid-2013, meant that (semi-) government services were less accessible to citizens. Care institutions and health insurers are also increasingly making use of DigiD as a trusted way for customers to access their portals. As a result, disturbing a single link can lead to serious disturbances in more than one vital process[6]. This example shows that suppliers and service providers are also part of the chain of dependencies and that they also have an impact on business processes.

Protection against such events goes beyond guaranteeing your own cybersecurity. In order to gain insight into vulnerabilities and risks, we must actively cooperate with our chain partners, suppliers and public parties. Cybersecurity and continuity issues are therefore increasingly on the joint agenda. But the step to actually taking action remains difficult. Because how does an organization know exactly on whom it depends (in terms of systems, processes or data)? Which critical ICT systems affect the chain? Who is responsible for them? What threats, issues and risks exist at the chain level? What effect does disruption have on the chain? And what measures should be taken jointly? So, the question is: who starts putting these issues on the agenda of all chain parties?

Arriving at the first step

In order to achieve good collaboration in the field of cybersecurity, organizations in the chain first have to investigate a number of themes. Various best practices are available on certain topics, such as FERM and Schiphol Group (Cyssec: Cyber Synergy Schiphol Ecosystem).

Mobilization
The first step is to contact and get to know the chain partners. Cybersecurity is a domain in which cooperation between public and private organizations, as well as between private organizations alone, is necessary to cope with the increased cyber threat. In order to get the parties moving, they need to look for common interests, such as joint services.

Chain responsibility
Responsibilities are complex issues that need to be discussed within the chain, which means that it is important to involve all parties. Agreements with suppliers, sub-contractors or customers who are part of the chain ensure that each chain partner's involvement is clear. Responsibility for a cybersecure chain does not depend on a single organization. Large companies can take responsibility for small businesses by setting the right example. Often, larger organizations have developed certain methods, while smaller companies do not have enough time and money to do so.

Mapping critical chains
The Cyber Security Council has ascertained that few companies and governments have sufficient overview of the digital chains on which they are dependent[7]. Insight into these chains is essential in order to identify risks and measures. According to the council, there is still too much emphasis in cybersecurity on the risks within the organization, and an integrated approach between chain partners is an important step towards improving security. To map these critical chains, it is important that relationships based on trust exist between the organizations when it comes to sharing sensitive information.

---

[1]De nationale Cyber Security Strategie Definitie, 2011.
[2]De nationale Cyber Security Strategie Definitie, 2011.
[3]Nationaal Cyber Security Cetrum: Cyber Security Beeld Nederland 2016
[4]Advies Cyber Security Raad, juli 2016.
[5]http://www.crimesite.nl/gehackte-haven-cokesmokkel-2-0-1/ 6CSBN, 2014.
[7]Digitale ketenveiligheid krijgt veel te weinig aandacht, Cyber Security Raad,11-07-2016 (https://www.cybersecurityraad.nl/010_Actueel/digitaleketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx)
[8]Cyber Security Supply Chain Risk Assessment methodology

Identifying joint risks
After the chains have been mapped, it is important for the parties identified to set clear priorities and focus on areas in which the risks are greatest (a risk-based approach). In addition, for chains that are part of vital national processes, new issues are raised, such as the role of the government and the need to share roles and responsibilities between different organizations. So, it is important that organizations in the chain develop and apply best practices themselves, to adequately protect the chain from the increased cybersecurity threat. For this reason, some companies in the energy sector have developed a methodology: the Cyber Security Supply Chain Risk Analysis[8].

Chain Impact
When organizations are transparent about their risks, it is important that the impact of a cyber incident to the chain can be assessed. A business impact assessment is already used by many individual organizations. Performing a Chain Impact Assessment (CIA) can give chains insight into the primary and supportive business processes, for example by mapping the dependency of an important ICT process and the consequences and impact of its possible failure.

Measures
Organizations that are part of a chain can best define the right measures and initiatives to reduce cybersecurity risks together with their chain partners. This requires actions from the (individual) organizations that are part of a chain or network. These measures can be implemented both within the business processes and within the systems. An example would be to jointly solve the top ten vulnerabilities.

Complex chains in an ecosystem

The establishment of cooperative chain networks is often complex. Two initiatives have been launched that focus on the so-called ecosystem: all of those dependent on different chains in an environment. The two initiatives, the Rotterdam Port (FERM) and the Schiphol Group (Cyssec), were both launched in 2016 to strengthen cybersecurity in their own ecosystem. These initiatives are supported by various public and private organizations, such as the National Coordinator for Terrorism and Security. They are public-private partnerships aimed at strengthening cybersecurity and, at the same time, exploring the economic opportunities of all parties associated with the ecosystem.

Taking the first step!
The first step that chains must take is to establish contact with all parties in an ecosystem and create awareness of the vulnerabilities, risks and importance of cooperation. Together, chains are more resilient. Taking the first step will eventually lead to a stronger chain.

About the authors

Kim van der Veen MSc is a consultant at Capgemini Consulting and focuses on the importance of human awareness in the context of cybersecurity. Evelien van Zuidam MSc is employed by Capgemini Consulting as a senior consultant and focuses on human, organizational and social issues in cybersecurity.


For more information, please contact the authors:
kim.vander.veen@capgemini.com, www.linkedin.com/in/kim-van-der-veen-3b4b494a and
evelien.van.zuidam@capgemini.com,
www.linkedin.com/in/evelienvanzuidam, @evelienvz

From web to WhatsApp

Intelligent IT improves contact between citizens and the police

Highlights

- Citizens choose which channel they use to communicate with the government
- The most popular social media channels in the Netherlands are Facebook and WhatsApp, so more contact with the police needs to take place via these channels
- Digital and artificial intelligence provide quick and accurate answers to questions and increase the value of contacts
- The use of social media channels as a means of communication promotes cooperation between agencies in the chain

Providing intelligent information through popular means of communication facilitates easier interaction between citizens and the police.

About five years ago, when the Dutch National Police was being formed, construction of the website politie.nl was started, as one face and one channel for Dutch citizens. More than 360 websites were integrated into a single website, making it a single channel on which all information could be found. But the way citizens use the internet is changing dramatically. Having a standard website is no longer enough. Obtaining information or reporting via forms is often the first sort of communication between citizens and police. But are forms still relevant in this day and age? In the Netherlands, WhatsApp and Facebook seem to be the most widely used communication channels. Websites are eclipsed by the amount of conversations conducted on such platforms. People are increasingly using communication tools like WhatsApp or Facebook to get information faster. In combination with Artificial Intelligence (AI), these tools can help people get faster and better answers to their questions.

Increased use of communication tools

Following the introduction of the landline in 1880, it took the Dutch population 125 years to reach 9 million connections[1]. The age of the mobile phone started around 1995[2] and it is estimated that there are now about 20 million of these in the Netherlands, more than the total population, in just 21 years' time. In 2016, the number of Facebook users[3] in the Netherlands was 9.6 million[4] (in 11 years) and for WhatsApp 9.8 million. WhatsApp achieved this number in just seven years.

The use of social media is also increasing, according to research into social media use in the Netherlands[5]. Media channels exist side by side and preferences for different channels change over time and vary according to age group and other demographic characteristics. Citizens choose for themselves which channel they want to use; companies and organizations no longer impose that. In 2017, one communication channel alone no longer suffices. If that's all you have, you will disappear in silence.

Popular platforms

It is therefore important for the police to make use of these communication channels. Giving every police officer access to WhatsApp or Facebook Messenger is not the solution. This would only shift contact between citizens and the police from the phone to the (social) media channel popular at that time. It is a precondition that the police should also be represented in the same virtual spaces inhabited by citizens, but it is not possible to continuously invest in switching to new platforms. For example, it would have been wasteful for the police to invest in the mainly Dutch oriented social network called Hyves in 2009, when it was popular. Hyves was surpassed by Facebook in 2011 and ceased to exist in 2013.

We need to be smarter than that. The starting point must be that the police are as represented in the virtual world as in the real world. The distribution of the most popular social media and demographics must take the lead in this; young people are now on Instagram and Snapchat. Social media use among those aged 65-plus is increasing, particularly on Facebook. The police must be able to move with the dynamics and shift their attention from one platform to another, and to newly introduced platforms, without it being a costly operation. Using the right techniques should make it easy to plug in to these platforms. Technically, this is already easily possible. The only question is: how will citizens benefit from this?

Valuable contact

In a "National Ombudsman" survey from 2016[6], the following top three public concerns are mentioned when contacting the government:

1. being sent from pillar to post by an official's ignorance
2. lack of clarity about the follow-up
3. Slow responses to questions

Digital intelligence (DI) may offer the solution. A chatbot can establish a dialogue with a citizen and ensure that they can navigate their way through the questions and answers. Using
a chatbot means less work for an employee. It gives the employee time to establish more valuable personal contacts with citizens. The chat can seamlessly move from a chatbot to a real employee. The quality of the answers therefore becomes better and more relevant, because routine referrals have already taken place. The citizen is led to the right place and gets the answers they are looking for.

Also, the quality of digital intelligence improves through use, as it is often possible to use AI solutions that apply machine learning. This means that the chatbot learns to improve itself during the dialogues it has with citizens. The chatbot displays the same behavior as an employee in conversations with citizens. In addition to using AI, a chatbot can also use Natural Language Programming. This is a specialization at the frontier of linguistics and AI; the natural language used by the citizen in the dialogue is analyzed by a computer to determine whether the question or answer can be better understood and a more appropriate response provided. The chatbot behaves more and more like a real employee over time and can therefore handle an ever-increasing number of routine enquiries.

Politie.nl is the medium through which Dutch citizens can find information on police-related matters. However, citizens do not always know who to ask a specific question, especially if it is not police related. In practice, questions which cannot be answered by the site are always answered by telephone. The service employee does not wish to disappoint the citizen or send them from pillar to post. Examples include reporting items found or stolen passports; reports that are actually intended for the municipality. In order to improve online service, deploying a chatbot helps to ensure that police questions are answered by the police and other questions by the relevant government agencies, without

[1] Number of fixed telephone connections in the Netherlands, Ad Blafhert, 2016.
[2] Column Annegreet van Bergen about the rise of the telephone, Historisch Nieuwsblad, 2016.
[3] Number of Dutch Facebook users anno 2016, Buzzcapture, 2016.
[4] Number of Dutch WhatsApp users anno 2016, Buzzcapture, 2016.
[5] National Social Media Research, Marketing Facts, 2017.
[6] Annoyances Research, Nationale Ombudsman, 2016.

the intervention of an employee from the relevant agency. The quality of citizens' contact with the government is hereby improved. Cooperation with other government departments is essential. The idea that each body uses its own method of maintaining contact is a thing of the past. Because citizens do not wish to contact a particular body; citizens simply want their problems to be solved immediately. In this way, DI helps citizens to receive the answer to their question immediately without having to start a search to find the right website, telephone number or government office. One example of this is the far-reaching cooperation in the digital criminal justice system for the benefit of improved victim care.

Developments in the field of IT never stop. Communication between citizens and between citizens and companies is constantly changing, with the choice of communication channel increasingly being left to the person themself. WhatsApp, Twitter, Facebook and Slack are currently the most important channels to support websites in their communication with citizens. The recently created New Media and Digital Services Program of the National Police is actively investigating the use of chatbots on police websites and WhatsApp and Facebook, which is part of the vision to be represented in the digital world in the same places as citizens. The program undertakes artificial intelligence (AI) activities to continuously improve its digital service, ease of use and quality.

About the authors

Sid B. Dane is a managing consultant at Capgemini and an Agile Coach, Scrum Master and Agile Project Manager. Jan-Willem van Doornspeek is a senior consultant and information analyst at Capgemini. In addition, he is actively working with Oracle

For more information, please contact the authors:
sid.dane@capgemini.com, www.linkedin.com/in/siddane and janwillem.van.doornspeek@capgemini.com, www.linkedin.com/in/jan-willem-van-doornspeek-2a12314

New times call for innovative security organizations

How do new organizational principles help to produce innovations?

Highlights

- New times call for new ways of working together
- Innovative Working is a way to make organizations more agile
- Various teams within the police are reinventing themselves and working innovatively
- New organizational principles are projects with a long lead time for which perseverance is a must
- The first results from teams applying Innovative Working have been encouraging, leading to increased job satisfaction and cost savings

There is clear consensus within the security domain that the speed with which society is changing produces enormous challenges. Solutions are mainly sought in dealing with data in a smarter way, better use of (cyber) technology, and creating more connections between organizations and citizens. However, we hear too little of the need for organizations to change the way they are organized.

We take the current method of organization as a given, with its hierarchy, control, departments, rules and procedures. Not a good basis for much-needed innovation. But there is hope that things can be different. Fortunately, there is a growing number of pioneers taking up the gauntlet and looking for new ways to work. Ways that respond to the ever-changing external demands and help to make innovation easier within the organization. They are engaged in the search for agility or, as we call it, Innovative Working. This article describes how new organizational principles can help to produce innovations and provides an insight into how the police apply them.

Organizations' search for agility and flexibility

The world in which we live is changing rapidly because of digitization, globalization and radicalization. This will change our work and the way we work with customers, citizens, partners, and executives. It also changes the pace at which organizations in the security domain must respond to such changes. This requires "maneuverability" within organizations.

However, many organizations are limited in their "maneuverability" by bureaucratic systems and procedures. These internal systems and procedures provide stability in a complex environment but limit the required flexibility of an organization in that same complex environment. Moreover, the more bureaucratic the systems are, the more complex they become. We are therefore solving the problem with its cause, which is illogical.

The search for agility and flexibility is a broad movement and many organizations go about it in their own way. Agile, Rijnlands organization, Scrum, Squads and Tribes are a few examples of new methods or new organizational structures.

Evolution of organizational principles

We consider this shift towards agility and flexibility primarily as an evolution of organizational principles; principles that guide how we organize the work. The common denominator is the shift from a fast-paced system world to a meaningful life world. From a system world based on returns, efficiency, control, and distrust to an environment based on trust, quality, time, attention and freedom of choice[1]. Within this movement, Innovative Working is a way to make organizations more agile. With Innovative Working, an organization moves away from focusing on control and systems, and focuses more on the reason for its existence. Wouter Hart, author of Verdraaide organisaties, terug naar de bedoeling (Backward Organizations: how to organize with the purpose in mind) calls this "aiming for the purpose".

- During the industrial revolution, the following principles dominated: standardization, specialization, synchronization, concentration, centralization and maximization[2]. In the current information age and networked society, we recognize new and complementary principles such as: digitize what can be digitized. Digitization as a continuation of standardization and synchronization.
- Agility calls for modular organization and assisted self-organization. Assisted self-organization as a continuation of concentration and centralization.
- People can create value by focusing on activities that cannot be digitized or are difficult to digitize for the benefit of others, such as designing or providing services[3]. Creation by people as a continuation of specialization.
- Added value is created by using and processing data. Enrichment with data as a continuation of standardization.
- With more powerful tools, work can be organized more flexibly in co-creation with customers. Co-creation in networks as a continuation of concentration and centralization.
- Implementation and innovation go hand in hand, based on feedback and insight into dynamics[4]. Continuous adaptation as a continuation of standardization, specialization, and centralization.
- People and organizations recognize, through intrinsic motivation and more publicity, that they are part of a larger whole. Contribution as a continuation of maximization[5 6].

Case: the police put Innovative Working into practice

For the police, Innovative Working has its anchor point in the needs stated in the National Police Realization Plan (December 2012) and the National Police Reformation Plan (August 2015). Both plans express a strong need to tackle more vulnerable (local) security problems and to do this from within an organization that is fully supportive.

This is stated in the Realization Plan's strategic goals:
1. Better police performance;
2. More legitimacy from and greater trust in the police and;
3. Function as a single entity

To achieve this, cultural ambitions have been formulated, which include in particular "More autonomy for the police professional" and "From accountability culture to organized trust" as ambitions that can be operationalized through Innovative Working. Meanwhile, many police teams (each with 100 to 200 full-time employees) have been challenged to reinvent themselves and become more flexible. They have been working innovatively. Innovative Working is working from the purpose; determining within your environment what you wish to achieve externally as a police team and adapting the internal work continuously to achieve this.

---

[1] Jan Rotmans, Verandering van een tijdperk.
[2] Alvin Toffler, on the industrial revolution in The Third wave.
[3] For further elaboration, see Klanthelden, excelleren in emotionele Klantbeleving
of Berry Veldhoen & Stephan van Slooten.
[4] This principle for example, takes shape in so-called Agile working, http://agilemethodology.org
[5] Another but somewhat similar summary is by Hans de Bruijne et al., Described in Nieuwerwets Organiseren naar aanleiding van een onderzoek in 2014 naar nieuwe organiseervormen in Nederland.
[6] Dirk Helbing calls for assisted self-organization and distributed management as essential organizing principles for dealing with complexity, in The Automation of Society is Next: How to Survive the Digital Revolution.

Step 1. Innovative Working has three main goals: better external results, more involved police officers and more efficient business operations. In this first step stakeholders, such as citizens, directors, employees, managers and partners, together set the team's Innovative Working ambitions. What do they consider good police work and with what results would they be pleased? The logic that must be realized between the goals, benefits and activities is recorded in a "benefit logic".

Step 2. Determine new organizational principles for how you wish to work as a team. Later in this article, we mention five principles that are often chosen. This reflects how current behavior fits these principles: where to do more, where less. It is also important to reflect on the meaning of the organizational principles for the team's current organizational form.

Step 3. Determine what you are going to do. Once the ambitions and principles have been established, employees formulate actions and further work is done to create trust. The actions are recorded in a route planner and on initiative cards, so that anyone can see and follow what's happening.

Step 4. Continuation of further development. Cashing in on the benefits, highlighting noticeable effects and learning what adds value in terms of better performance and what is unnecessary[7]. In short: learning from their own experiences in daily practice.

Each team is unique and has its own unique context, but the search for innovation basically follows four steps, as described on this page. This approach has taught different (basic) teams how to get a better idea of what the team wants to achieve externally and which organizational principles are suitable and lead to further improvement initiatives, such as on-site reporting, police involvement in networks, mobile working, small self-organizing teams, self-scheduling and working from the town/city hall. These teams followed the same approach to arrive at innovation but it should not be seen as a blueprint. Each team has its own dynamics, context and issues. It is a process approach, a roadmap, which always produces different outcomes. Thus, the teams have to think for themselves to make the approach their own. The police professionals shape the approach itself through management support and in collaboration with the local community. This implies the cultural ambitions of striving for more professional autonomy for police officers/detectives and more control and trust. Based on these needs, the previously described evolution of general organizational principles and the experiences of the teams to date, five principles have been distilled for police teams.

1. **Extern samenwerken**
   External safety cannot be guaranteed by a police team alone. It is necessary to cooperate and co-create with citizens and other parties both outside and within the police organization. In addition, take the time to build personal relationships, ask what others are happy about, establish goals, exchange information, let them know what's happening and provide feedback on agreements made. This leads to local and problem-oriented work from the viewpoint of being vigilant and providing a service.

2. **Feeling responsible**
   Certainly, in local police work, people can make the difference. Characteristics such as feeling, compassion and the ability to improvise are decisive. In order to contribute to the "purpose", you must organize what you and your immediate colleagues are responsible for: what external safety, for example, and for which area or problem. In addition, the basics must be in order: you must be able to work safely, have recognizable social relationships and have executives who support you in difficult times. Managers must understand that difficult decisions have to be made that sometimes lead to the wrong outcomes. The result is involved people who feel responsible for good police work. Based on this organizational principle, many teams have taken the step to become self-organized in small (geographic or thematic) sub-teams of 20-25 full-time employees.

3. **Good police work[8]**
   It is all about professional work on a daily basis, whether or not on the street, during which results are expected. What

does professionalism mean? Making and using space and, where necessary, breaking through anxiety and hierarchical culture. But also talking to each other and getting problems and annoyances out in the open, taking responsibility for your actions, and reflecting on the police values of connecting, trustworthiness, courage and integrity. Providing added value by making use of new digital capabilities. Not only sharing experiences freely, but going full circle.

4. **The appeal of the imagination**
   People are narrative creatures and this applies to police officers in particular[9]. In order to keep working from the goal, it is necessary to put the desired outcome into words and experience it in a way that is appealing[10]. That's something very different from hard facts, rational analyses and professional insight. It is also about making the image of police officers appealing and arriving at a living, credible story. Innovative Working is for and by colleagues who inspire each other and come up with new ideas.

5. **Self-experimentation**
   In order to keep up with the dynamics of their surrounding communities, it is important for teams to continuously refresh themselves. This involves experimenting with new technologies and approaches, whether or not as a pilot for national developments. As a result, Innovative Working can take the form of small steps and consistently better results can be achieved externally.

Assisted self-organization in teams requires different support

As more teams take up Innovative Working, it becomes necessary to think about what this means for the rest of the organization; the management, the pillars, and the business. In order to help in answering these questions, the authors of this article have formulated five additional organizational principles.

1. **Create spaces for teams**
   In order to give added meaning to the work in interaction with the surrounding community, a modular organization with assisted self-organization is helpful.
2. **Share business operations effectively**
   Standardizing and, to a lesser extent, centralizing and concentrating make it possible to collaborate effectively and efficiently[11].

[7] Louis Cauffman, Simpel. Over progressiegericht werken.
[8] The term good police work refers to the work of Jan Nap about richer accountability amongst others.
[9] Merlin van Hulst, Politie verhalen, een etnografie van een belangrijk aspect van politieculturen.
[10] Gabriël van den Brink. Hoe wij beter over kennis kunnen nadenken.
[11] Hans Strikwerda, multidimensional organizations.
[12] Principles of Rhine, make of that what you can.

3. **Make joint decisions on matters that affect other teams**
   It's about "deciding with" instead of "deciding for" and mobilizing the available knowledge to arrive at good decisions[12].
4. **Ability to scale up and down**
   The work is organized among existing teams, unless that is no longer possible or convenient. Then a new team can be set up, a team can be disassembled, or a collaborative construction can be built under the direction of one or more teams.
5. **Make wise agreements**
   Work in a calmer and more reflective way with rules and frameworks. In addition, present the agreements attractively and accessibly.

By applying these organizational principles, an organization of professionals can be created; one which enjoys working on safety in a networked way and feels supported by adequate business practices and meaningful agreements.

What can we learn from the police?

The first results from teams practicing Innovative Working are encouraging. External results have noticeably improved, job satisfaction is higher, due to increased corporate ownership, and even cost savings seem to have been realized through the reduction of traditional housing and workplaces. Nevertheless, it requires perseverance, (change learning) help and support from the surrounding community. Realizing this social innovation within a team requires executives who realize it is a marathon and not a sprint. And the realization that more facilitation management is needed, by managers who dare to discuss current practices. Since the outcome is uncertain, it helps to make the first steps predictable. Also, some help in concretizing the first improvement initiatives helps to book the first small successes.

We can also learn from the police that it helps to discuss and establish the above organizational principles per team. Each team creates its own organizational principles with its own language. But the above organizational principles are appropriate and sufficient. They stimulate dynamism but also have stabilizing elements, suitable for a social system.

A wonderful lesson is that Innovative Working also deserves another method of accountability. A method of accountability that is more appropriate for the complexity of the work than the current, often quantitative, accountability of the results. We call this Richer Accountability; a form of accountability that is better suited to the government's philosophy of "New Public Governance".

Elements of this method of accountability include: multiple perspectives versus results achieved, more horizontal accountability to the community, rather than vertically to the boss, more narrative in dialogue with the community and more continuous dialogue, instead of periodically. Both the police and care agencies are currently experimenting extensively with richer forms of accountability. A fascinating endeavor.

Finally

We started this article with the call to adapt the way in which security organizations are organized to meet the demands of an ever-changing society. The search for agility is widely discernible in many organizations but still limited within the security domain. We see this search as an evolution of organizational principles. The police are trying out new organizational principles and learning from their experiences. This article is too short to do justice to the depth of organizational development within the police. However, this brief insight teaches us that it is not rocket science, and that it is significantly beneficial, contributes to greater external safety, greater well-being within the organization, and efficient business operations. We hope that this insight will be seen as an invitation to make a start yourself on working towards Innovative Working. How can your organization work more with the purpose in mind, better align with the changing outside world and continuously refresh itself internally? Our advice: start small and let it grow viral.

About the authors

Erik Staffeleu MSc is a business consultant, principal consultant and Head of Transformation Program Management. Volken Timmerman MSc is an independent organization adviser. Both are active as organization advisors and change experts in the security domain. Their particular specialty is the guidance of transformations and the realization of visible changes.

For more information, please contact the authors:
erik.staffeleu@capgemini.com, www.linkedin.com/in/erikstaffeleu and contact@volkentimmerman.nl, www.linkedin.com/in/volken-timmerman-33854b

Face off! The use of biometrics in efficient applications is contributing to state security

To what extent is the growing number of biometric applications for more efficient border controls a source of information for investigations in the fight against terrorism?

Highlights

- Use of biometric applications in the fight against terrorism
- Opportunities for biometric applications to make travel more efficient
- The importance of a good balance between travel efficiency and safeguarding privacy

The increase in social concerns that has risen in the last few years, caused by terrorist attacks, has led to a need to control boundaries more strictly. The use of biometric data plays an increasingly important role. This article describes the need for biometric applications to improve state security, highlights some biometric trends, and provides a glimpse of the future in terms of impact and opportunities.

The need for biometric applications

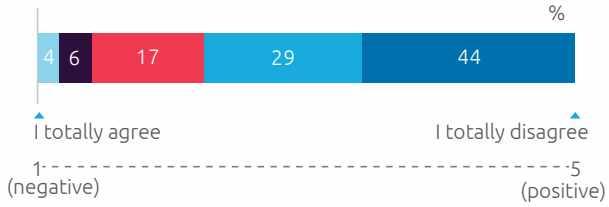
Istanbul and Paris, among others, still fresh in our memory, all available measures are being taken to identify unwanted and potentially dangerous travelers at the border. We want to know who has arrived in a country and when, and if travelers have left the country again. To make this possible, the Schengen Borders Code has been adapted. Now, both citizens of the European Union and non-EU citizens must undergo a systematic security check when they enter or leave the EU. Anyone entering the European Union via external borders undergoes database searches, such as in the Schengen Information System (SIS) and the database on lost and stolen travel documents. As well as EU citizens, travelers from around the world are also checked. To ensure the best possible security, at Schiphol Airport certain procedures for checking passengers and their luggage are being used by the National Coordinator for Terrorism and Security (NCTV).

In this way, border control technologies based on biometrics are helping to maintain state security.

Development of biometric applications

AFor years, the use of fingerprint technologies has been popular. Currently, we are seeing a shift to other forms of biometrics, such as iris scans or facial recognition. These technologies are used to gather information on individuals to increase the security of society and the state. This increase in other forms of biometric verification ensures that security services are provided with more information to detect and track suspicious persons. Smart cameras have been deployed in many places (such as train stations, airports and border crossings) to map the environment thoroughly and identify suspicious situations sooner. Our society supports measures. According to research by Kantar TNS, only ten percent of Dutch people are negative towards the use of biometrics at border controls.

Figure 1: What do you think of the (possible) use of biometrics at border controls to increase your security?



Current initiatives

In addition to increasing state security, these technologies also make certain processes more efficient, such as border controls. More and more airports allow travelers to pass through the various controls without a boarding pass and/or passport. The controls that take place are carried out based on facial recognition. Some examples of current initiatives for the application of biometric data at border controls include:

1. At US airports, customs now use special systems that make use of face recognition. Through scanners, a traveler's face is compared to the photo on their passport. Links with police systems enable the scanners to show if someone is using a false ID.
2. As part of the US VISIT Biometric Entry and Exit program, border crossings between the US and Mexico are equipped with fingerprint and iris scanners. This technology has already been tested successfully at border crossings between Afghanistan and Iraq.
3. With the Schiphol NeXt program, the Dutch airport is attempting to make security more effective by using smart cameras and robots to detect people behaving suspiciously.
4. With Aruba Happy Flow, public border control is linked to private passenger data to make the passenger process fast, safe and easy.
5. By 2020, Australia's Seamless Traveler project aims to allow 90% of its passengers to pass through its automated passenger process, which makes use of biometric features.

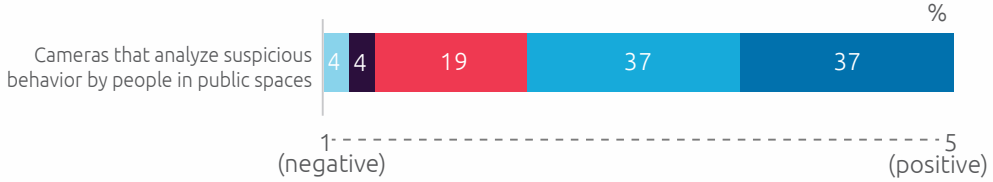
These initiatives have in common that they record and verify travelers' biometric features when crossing a border by land or air. In addition to the state security interests served in this way, it also offers great benefits to travelers. For example,

waiting times at customs and passport checks are drastically reduced. In addition, the risk of theft of identification papers is reduced because travelers can safely store them after showing them only once.

Safety and convenience aspects

The examples of biometric technologies described above, are often mentioned in the same breath as the management of threats to society. In addition to the need for these technologies in the fight against terrorism, they also offer many opportunities for travelers. The success of initiatives like Aruba Happy Flow and Schiphol NeXt is due to a combination of many factors. The initiatives make it possible to work more efficiently, reducing the number of staff, passengers do not have to show their travel documents multiple times, and they are more confident in the fact that close monitoring is being performed. The applications make it possible to track people at airports from the moment of entry to departure. This offers possibilities for enforcement and detection purposes. And society supports these measures. Research by Kantar TNS shows that seven out of 10 Dutch people are in favor of the development of tools, like body cams, biometrics and cameras with face recognition in public spaces, to increase security.

Figure 2: What do you think of the (possible) use of the technologies below to increase your security?



With state security as a higher goal, biometric data is (or may be) combined with different data sources. This includes using sources such as Automated Number Plate Recognition (ANPR), Closed Circuit Television (CCTV), Passenger Name Records (PNR), as well as police sources, which are combined with passenger biometric data (like the fingerprint in your passport). Combining different data sources with biometric data brings enormous opportunities for passengers and airlines, but also for detection and enforcement. For example, tracking a missing child (at an airport), tracking people who checked in their luggage but are not at the gate in time, connecting people to unclaimed luggage, but also commercial opportunities, such as displaying the right ad to the right traveler. Use of data analytics can provide insight into travelers' airport movement patterns, purchasing preferences, or to predict those travelers likely to delay a flight. Analysis of these combined data sources can also reveal patterns of people who behave differently and people with criminal or terrorist intentions. Theoretically, analyzing travelers' behavior can benefit both the individual's ease of passage, as well as individual and overall safety.

Risks

Although we are happy to facilitate the smooth flow of traffic during our trip, this involves some important safety issues. In addition to the range of opportunities offered by biometric technologies, there are also privacy and security issues. When using personal data, it must be strictly examined whether the use of those data is proportional to the purposes for which they were collected. In addition, transparency about the data collection is important and sometimes permission is required to process data. Furthermore, biometric properties are unique, but this does not mean that they are not hackable. It has already been shown that biometric facial features can be "hacked" through plastic surgery and a plastic fingerprint can even be made based on a high-resolution image of a real fingerprint. The desire to regain control over borders is leading to countries increasingly taking measures to gain insight into who crosses borders, along with when and where. Applications using biometric verification are increasingly being used to identify suspects. In addition, we see that biometrics are offering travelers at airports the opportunity to avoid the inconvenience of the usual controls. In both cases, a passenger's biometric features are used.

Whether the use of these applications actually leads to a safer situation remains to be seen. It will certainly result in a shift in the trade-off between security and privacy. Whether, and to what extent, we are prepared to give away more and more privacy in return for a stronger sense of security, and for applications that make our lives more efficient, are important questions that we must continue to ask ourselves.

About the authors

Gijs Daalmijer MSc is a public administration and security expert and consultant at Capgemini. He is active in the field of public safety and security with a special focus on biometrics. Lieke Schepers MSc is a criminologist and senior consultant at Capgemini. Lieke focuses on issues in the public safety and security market, especially intelligence and digital forensics.

For more information, please contact the authors:
gijs.daalmijer@capgemini.com
and lieke.schepers@capgemini.com

Sensing in the connected society - three opportunities for public safety

In what ways can everyday smart objects help to increase the safety of society?

Highlights

- Public spaces can be managed in real-time, based on sensors
- Data analytics creates a manual for preventive enforcement
- No sensing in a connected society without good security for any connected object
- Transparent use of sensor information offers added value while privacy remains controllable

It's a cliché but technological developments such as self-driving cars, robotics and smart cities, are happening in a fast manner. These are concepts from science fiction movies that you can see in real life today. The prediction of former Intel® chairman Gordon Moore in 1965 that the power and capabilities of (computer) chip technologies will double everyone to two years has more than come true[1]. The exponential increase in technological capabilities offers huge opportunities for industry, consumers, but above all for the public sector in the challenge of in creasing public safety. In this article, we focus on three applications of sensing, which we consider to be most valuable for increasing public safety, namely: proactive enforcement of public spaces, crowd management and improved crime detection. These applications create the obligation to handle security and privacy with the utmost care.

Technological developments in the field of sensing are to a large extent due to ever-smaller chips with greater computing power, which are also very energy efficient. This enables everyday objects to be fitted with sensors and by doing so are made "smart". These sensors detect their surrounding environment (which is called sensing) and can communicate with other objects. In fact, these sensors can measure everything and generate massive amounts of data (Big Data), which makes analytics crucial for gaining the right perspective for action. We call the network of interconnected smart objects the "Internet of Things" (IoT). Research by Kantar TNS shows that the use of such technological tools is a positive development in terms of safety by around 7 out of 10 Dutch people.

Internet of Things

As previously mentioned, some science fiction is no longer fiction. In addition to developments such as nanotechnology, robotics and 3D printing, the IoT plays a significant role. The dense network of sensors within the IoT is created because more and more (everyday) technologies are connected to the internet. Several definitions of the IoT are described in literature. Most definitions consist of the following elements:

1. Sensors that collect data.
2. Data and communication technology built into physical objects.
3. Connected to a network or the internet: physical items are no longer separate from the virtual world, but can be controlled and behave as a physical access point to internet services.

IoT creates a world in which objects can automatically communicate with computers and each other, to provide services that benefit mankind. For example, car manufacturers are working on allowing cars to communicate with smart traffic lights to improve the traffic flow in city centers. Or the smart traffic light can adjust its pattern to suit the amount of traffic waiting at the traffic light[2]. But it doesn't end with smart traffic lights. Sensors are also being added, for example, to trash cans (indicating when they are full and ready to be emptied), road signs, parking lots and bicycle stands, drones, self-driving cars and mobile phones. The IoT is currently booming in society. By generating data on public spaces, based on a dense network of sensors, we can anticipate the modern challenges to the safety, liberty and quality of life in our cities. Sensors are able to sense the situation in public spaces, for example, and (continuously) measure it; both the environment (for example, pressure, air quality and sound), as well as specific objects (availability of bicycle stands). These measurements and their real-time availability can show if the situation is within, above or beyond acceptable limits. By placing these data in historical perspective, trends can be determined that can also be predictive or indicative of the future. The real-time use of this data and linking it with all kinds of resources makes it possible to manage the public space.

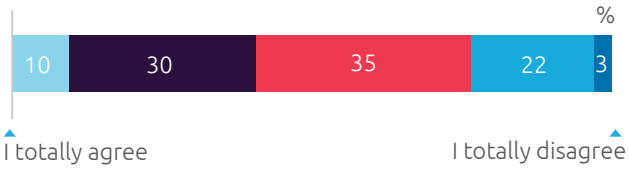
We see three very valuable applications for improving safety:

1. **Proactive enforcement of legal standards in our habitat**
   In light of the new law on the public habitat in the Netherlands, outdoor sensors can play an important role in the efficient and effective maintenance of the public habitat and providing permits. Large-scale analyses of a multitude of data generated by sensors enable new insights to be gained concerning compliance with legal standards, such as air or soil quality. Based on trends in data, we can predict that the quality of air at a factory will deteriorate. Whereas this was previously dependent on regular inspections, air quality can now be measured all year round, 24 hours a day. Chemical disasters, such as the one at Chemie-pack in the Netherlands in 2011, and thus widespread public health consequences can be prevented. Preventive enforcement only takes place when legal standards threaten to be exceeded. Thus, the policy maker's costs for implementing a reactive policy can be further reduced and citizens will experience as little nuisance as possible. By receiving sensor data, it is not always necessary to monitor situations through an inspection. This saves the government money, and perhaps our society as well.

2. **Measuring and predicting crowded periods in inner cities enabling visitor flows to be better managed**
   The Netherlands is popular among tourists. The country will receive an estimated 16 million visitors a year by 2020, of which a large proportion will visit our capital, Amsterdam[3]. It is estimated that Amsterdam[3] will soon receive around 20 million visitors a year. This leads to increased inconvenience for residents and takes up a lot of police[4] capacity.

The police have already warned that Amsterdam is becoming too crowded and has even preventively closed the main street Kalverstraat several times because people were no longer able to leave the shops they were visiting. Research from Kantar TNS shows that, in addition to the police, about half of Dutch people experience extreme crowding as unsafe.

Figure 1: Physical crowding in inner cities has a negative impact on my sense of safety.



[1]https://nl.wikipedia.org/wiki/Wet_van_Moor
[2]http://nos.nl/artikel/2133816-slim-stoplicht-in-rotterdam-voelt-hoeveel-fietsers-er-staan-te-wachten.html
[3]https://www.rijksoverheid.nl/actueel/nieuws/2015/04/23/toeristen-besteden-ruim-10-miljard-euro-aan-bezoek-nederland

The growing number of cameras in outdoor areas creates an increased sense of safety. Whereas a large amount of people (crowds) are seen as a challenge, a large amount of digital data contributes to a solution to those crowds. The current system for monitoring crowds in Amsterdam is still limited and based on cameras[5]. In addition to cameras, sensors in objects can also measure overcrowding. Combined with tourist flow data (hotel bookings, flights, public transport, etc.), these sensor data can provide a very immediate insight into urban crowding. Analysis of this data stream provides opportunities to better distribute the tourist stream across the city and its surroundings. By providing these insights to tourists in the form of routing advice through mobile apps and other means of communication (for example: "for a good experience, go to the Johan Cruyff Arena and not to the Kalverstraat"), safety can be improved.

3. Dense network with possible traces for crime detection

The data generated by sensors are also expected to provide great opportunities to improve the detection of crime. In fact, the dense network creates a great deal of additional digital evidence. Combined with sensor data from officers and citizens' mobile phones, a crime scene can be very accurately reconstructed. A striking example is a murder case in which Echo, a smart home assistant from Amazon, witnessed a suspected murder. Echo's "testimony", i.e. what the device heard and stored, will be used to prove the guilt or innocence of the accused. Another example is that, in addition to video surveillance, sensor data (bodycams, mobile phones) and cars (dashcams, connected car, self-driving cars) can also be used to obtain a much more intricate and complete picture of a crime scene. Data from such sources can, on the one hand, increase the red-handed power and, on the other, contribute to preventive enforcement in order to prevent criminal offenses. Based on data analyses of the IoT data obtained and the predictive and prescriptive analyses resulting from this, a kind of handbook for enforcement is created. In theory, this development means that there will be no blind spots in the surveillance network. In practice, it means that the police have the "eyes and ears" in places where they previously did not. In addition to this great potential, there are two crucial aspects that are important to the carefree application and exploitation of the enormous potential of IoT technology.

Security

The FBI already warned in 2015 that the application of IoT requires awareness in the area of security. If this is not properly applied, cyber criminals will be in a position to exploit weaknesses in an IoT system. On October 21, 2016, IoT was abused in the biggest cyber attack in the history of the internet on Twitter, the Wall Street Journal, Netflix, Reddit and Spotify[6]. This attack was carried out via, among other things, smart lamps, ovens and video recorders, without the owners being aware of it. Research by Kantar TNS shows that more than half of Dutch people are concerned to insufficiently secured technologies that are connected to the internet. The aforementioned attack was still relatively innocent, but it would be quite different if a serious attack were to take place, perhaps involving a city's traffic lights being disrupted by hackers or a smart home whose rightful owner is locked out or even attacked by smart objects because their house has been hacked. Theoretically, any object connected to the IoT (and thus the internet) is hackable. It is therefore of the utmost importance that the IoT's application in improving public safety only takes place when the security of each connected IoT object is well-organized. The security of the IoT is only as strong as its weakest (IoT object) link.

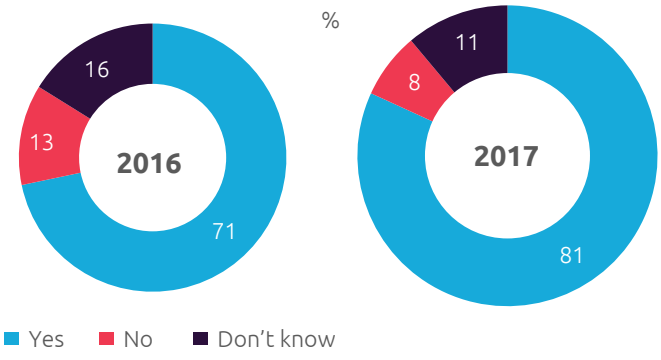
Figure 2: It worries me that more and more insufficiently secure technologies are connected to the internet (such as thermostats, smart meters, lights, alarms and smart TVs).

[4]https://www.nrc.nl/nieuws/2017/04/13/drugshandel-wint-terrein-inhoofdstad-8213415-a1554597
[5]https://www.nrc.nl/nieuws/2017/04/13/amsterdam-wil-de-massaswegmasseren-8213817-a1554618
[6]https://www.theguardian.com/technology/2016/oct/21/ddos-attackdyn-internet-denial-service

Privacy

Although technological capabilities are increasing, confidence in the safe and honest use of data is decreasing. Privacy is also an extremely important issue in the Netherlands, especially now that the European General Data Protection Regulation is coming into force in 2018, which will sharpen privacy requirements throughout the European Union. Depending on the purpose of the IoT network, sensors often measure their surroundings and generate data that cannot be traced back to individual persons. As a result, there is no theoretical breach of the privacy of these individuals. Sensors should hold this line as much as possible. However, certain sensor data, for example in combination with data from a car or mobile phone, can be traced back to an individual. In such cases, compliance with the Personal Data Protection Act and the Police Data Law must be verifiable for the citizen. Despite the privacy implications of the increase in data from smart objects, research from Kantar TNS shows more than 80% of Dutch people think that these data may have a positive impact on crime investigation opportunities. In addition, it is especially important that transparency is provided in applying data analyses to the massively generated data from IoT objects. Monitoring the applications and understanding the insights gained will ensure lasting confidence in these technologies.

Figure 3: Eight out of ten Dutch people are convinced that the increase in information will lead to greater opportunities for investigating crime.



The potential of new technologies like sensing is so substantial that preventive action becomes a real possibility. Analytics are therefore a critical success factor in gaining a concrete action perspective based on Big Data. The increasingly confirmed prediction of the future shows that in our society more co-creation is taking place between citizens, government and the private sector. Confidence and open data are playing a major role in this. In addition, security and privacy conditions are very important to exploiting the potential of these technologies. However, with close supervision, the opportunities created by new technological developments like the IoT do not have to be overshadowed by their threats.

About the authors

Martijn van de Ridder MSc works for Capgemini Insights & Data. Martijn is a principal consultant in the field of (Business) Intelligence, Big Data & Analytics, focusing on the public safety and security market. Lieke Schepers MSc is a criminologist and senior consultant at Capgemini. Lieke focuses on the field of public safety and security and specializes in intelligence and digital forensics.

For more information, please contact the authors:
Martijn.vande.ridder@capgemini.com,
www.linkedin.com/in/Martijnvanderidder
and lieke.schepers@capgemini.com,
Www.linkedin.com/in/liekeschepers

Access to billions of devices: a new risk!

Protecting devices through Identity & Access Management

Highlights

- More and more connected devices are being used. The importance of and dependence on these devices is growing
- Devices are often simple computers with limited memory and computing power, and should be treated accordingly from a security point of view
- Safety measures for devices must be taken based on standardized risk analysis, considering the characteristics of the devices
- Identity & Access Management (IAM) is a proven mechanism to secure devices against abuse, failure, fraud, intellectual property infringement, and invasion of privacy
- For end users, IAM should be as simple as possible when using devices

In many sectors, such as the energy, health, automotive and transport sectors, more and more interconnected devices are being used. The Internet of Things (IoT) is an example of this. The different types of devices used are extremely diverse and range from servers, wearables, smart meters and pacemakers to autonomous robots. These devices can exchange data and make use of each other's functionality. The scale on which devices are used, the importance of their usage to mankind and the information being exchanged are constantly growing. More than 55% of Dutch people believe that the Dutch government and companies are insufficiently prepared for a possible cyber war[1]. How do we ensure that attacks are prevented and that large numbers of connected devices can be safely included in the IT landscape?

Figuur 1: More than 55% of Dutch people consider that the Dutch government and companies are insufficiently prepared for a possible cyber war.

The Dutch government is sufficiently prepared for a possible cyber war.

Dutch companies are sufficiently prepared for a possible cyber war.

An essential and proven way to secure access to systems and information is Identity & Access Management (IAM). In the past, IAM focused on people, such as employees and customers, but IAM can also be applied to devices.

A cybersecurity strategy for devices is necessary

When developing devices, the focus is often on ease of use and short time-to-market. Security is often a secondary consideration, which means that the devices contain many vulnerabilities. This creates new attack possibilities for cybercriminals and other malicious parties, on a scale we have seen never before. To prevent abuse, failure, fraud, infringement of intellectual property and invasion of privacy, it is necessary to choose a good strategy for using devices securely in business processes.

The attack on the internet company Dyn[2] by the Mirai botnet illustrates how devices can be abused. Twenty Dyn data centers were attacked by a network of infected devices, resulting in (temporarily) unavailable services. As a result, Twitter and Soundcloud, among others, were not accessible. Mirai focuses on different sectors and, in addition to websites, on physical infrastructure[3].

Developments: more and more connected devices

Gartner has predicted growth from 6 billion connected devices in 2016 to 20 billion by 2020[4]. A number of developments is stimulating this growth. Ever-increasing digitization, for example, leads to more and more processes being carried out automatically and autonomously. This creates new possibilities and enables cost reduction. In addition, it is becoming increasingly important to have real-time information. In health care, it can save lives if a doctor has real-time and remote information on the heart rate and blood pressure of a patient. The IT landscape is becoming increasingly heterogeneous and the boundary between IT and the rest of the organization is fading. Devices have more sensors whose data can also (partly) be shared with the supplier, for example, to perform timely maintenance. As Mikko Hypponen, leading security expert, said, "In five years' time, if you go and buy a toaster – regardless of the toaster you buy, even if there's no IoT features – it's still gonna be an IoT toaster. It's still gonna call home to the manufacturer[5]."

New legislation and regulations

Developments in legislation and regulations are forcing organizations to form policies for the use of connected devices. One of these developments is the European General Data Protection Regulation (GDPR). The GDPR, which comes into effect in May 2018, requires organizations to clarify which data are located in the organization and where they are used. This means that an organization must also know on which devices customer and company data is stored.

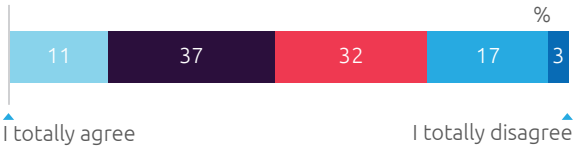
[1]TNS Kantar - Trends in Veiligheid 2017 - Onderzoek onder de bevolking
[2]https://tweakers.net/nieuws/117059/ddos-aanval-op-dns-provider-dynwerd-uitgevoerd-met-mirai-botnet.html en https://dyn.com/blog/dynstatement-on-10212016-ddos-attack/
[3]https://www.rathenau.nl/nl/publicatie/een-nooit-gelopen-race
[4]https://www.gartner.com/newsroom/id/3165317
[5] http://www.businessinsider.com/internet-of-things-invade-your-homemikko-hypponen-interview-lg-nest-revolv-2017-1?International=true&r=US&IR=T

The rise of the API economy

The importance of communication between devices is also growing with the emerging "API economy". An API is an interface over which software can communicate. By using APIs, it is no longer necessary to use a service provider's user interface and services can be called directly. This creates an ecosystem in which all kinds of device can make use of each other. Some companies have also standardized the provision of APIs internally.

A good example of an API economy development is the Payment Service Directive 2 (PSD2) within the financial sector. PSD2 states that services currently provided by banks can also be delivered by third parties. In theory, these transactions can then be carried out automatically by devices. If devices act on behalf of an individual, that individual must grant their permission for it to do so, also called consent. This has consequences for human beings. Research[6] shows that nearly half of people are concerned about losing control over devices.

Figure 2: I am worried about humans losing control over machines that interact and communicate with each other (such as robots that can think for themselves).



Threats, vulnerabilities and possible consequences

It is important for devices to understand the threats, vulnerabilities (the threat of abuse) and risks involved. Devices are simple computers with a processor, memory, network connection and software. Inadequate verification of identity (authentication), too many authorizations, and not changing the default password[7] are important vulnerabilities. More hardware-specific vulnerabilities include: implicit trust between devices, not registering devices, uncontrolled disposal of devices, lack of secure update mechanisms, hard-encrypted passwords, web interfaces that contain known vulnerabilities and easy-to-crack security codes[8]. Such vulnerabilities can, for example, be abused in the following ways:

- The configuration can be adapted without authorization.
- The hardware control software (firmware) may be overwritten without authorization.

- The device can be infected with malicious software (malware).
- Security codes can be stolen from the device to enable abuse.
  Most forms of software security can be bypassed if you have physical access to a device. A device that is not physically secure is vulnerable. A poorly secured device can be an entry point to the rest of the network for an attacker. When a device is lost or stolen, it is therefore important to deny access to the device.

Actors and their impact

What constitutes a threat depends on the type of organization that owns the devices. Possible examples include (professional) criminals, (activist) hackers, terrorists, (hostile) governments, competing companies and employees. The degree of threat and its impact partly depend on the number of connected devices. Examples of the possible impact the aforementioned actors can cause include:

- (Partially) unavailable services due to a DDoS attack. The current DDoS[9] attacks can generate so much internet traffic that is difficult to defend yourself.
- Unauthorized access to services can lead to leakage of privacy-sensitive information. For example, the hacking of smart TVs[10].
- A device can impersonate another device. This allows malicious parties to change data unauthorized or commit fraud.

[6] TNS Kantar - Trends in Security 2017 - Survey among the population
[7] https://www.capgemini-consulting.com/resource-file-access/resource/ pdf / securing_the_internet_of_things.pdf
[8] https://www.owasp.org/index.php/IoT_Attack_Surface_Areas
[9] Distributed Denial of Service (DDoS) is the name for a type of attack that makes a particular service (for example, a website) unavailable for its usual customers. A DDoS is often executed by destroying the website with a lot of network traffic, making it unattainable. "Cybersecurity image The Netherlands CSBN 2016.

Device challenges

For devices, just as with simple computers, the threats are not new and risks can be managed in a business-as-usual way. However, there are a number of specific challenges that IAM needs to take into account for devices.

Devices are not "standard" IT

Currently, devices are often not seen as "IT" and therefore do not form part of standard IT processes. They are put to use without the IT department being involved. The number of devices involved and the expected growth make this a huge challenge.

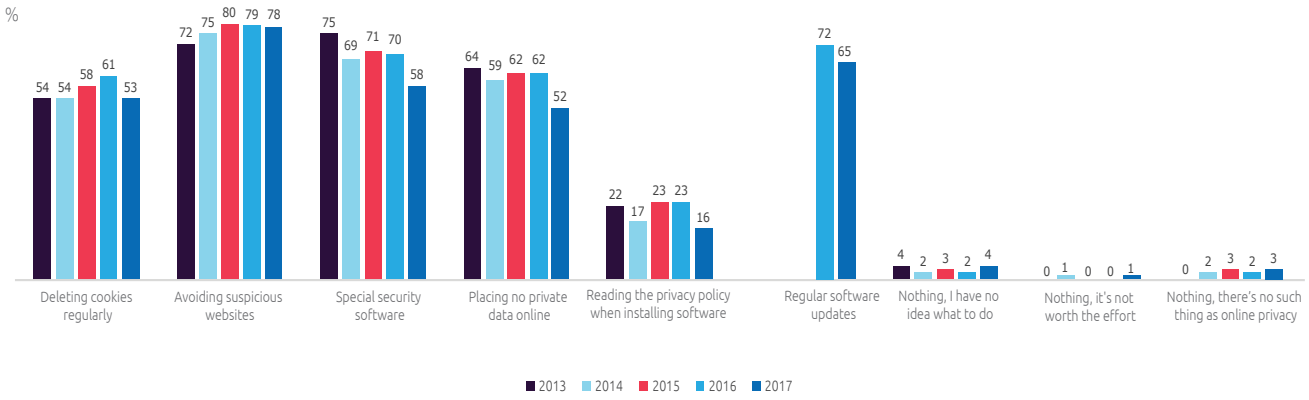
Boundaries of the internal network fade

More and more devices are being used outside of their own network, but are nevertheless connected to their own network. Whereas in the past you could impose strict limitations between networks and responsibilities, now an integrated chain approach is necessary. A chain is only as strong as its weakest link. Certainly, if the chain extends across multiple legal entities, suppliers, clients and/or customers, this represents an additional challenge.

Lack of (latest) security updates

Many IoT devices do not come from the IT world. This means, for example, that the baseline security measures that are a standard part of traditional IT are not included. For example, it is not always the case that a vendor makes security updates available and the vendor often has no mechanism to distribute updates automatically[11]. As a result, (known) vulnerabilities in systems remain in existence over long periods. This while the regular updating of software is one of the most commonly used measures to prevent abuse.

Figure 3: Regular updating of software and avoiding suspicious websites are the most-used methods to protect privacy.



[10] http://nos.nl/artikel/2161789-wikileaks-cia-used-smartphone-en-slimme-tv-for-af listening.html

[11] https://www.consumentenbond.nl/acties/updaten/nauwelijks-updates-naar-android-6.0 12 TNS Kantar - Trends in Security 2017

One step ahead: Protecting devices with IAM

To protect against threats, appropriate measures must be taken. The lessons learned in information security over the past twenty years can also be applied to devices. When defining and introducing measures, the specific challenges for IAM in relation to devices should be considered. It is impossible to be fully protected against all threats because each organization has limited resources. It should, therefore, be considered against which threats you want to be safeguarded based on a risk assessment. The highest-risk threats and vulnerabilities can be dealt with first by avoiding, reducing, transferring or accepting the risk.

Create awareness

First of all, awareness must be created of the need for device security. This awareness ensures support when taking measures. Acknowledging and creating awareness of the challenge is, therefore, a crucial prerequisite for protecting devices with IAM.

Verify the identity of the device

Before a device can access data, the device's identity must first be verified. Registration of the device, its identity and to what the device has access to, is necessary. For end users, the use of devices must be as easy as possible.

Take large numbers of devices into consideration

Many existing IAM systems are designed for smaller, relatively stable numbers of employees and/or customers. The number of devices will increase rapidly and potentially reach far greater quantities than have been managed up to now. The design of an IAM solution should, therefore, take into account large numbers of identity verifications, session validations and access controls. In order to keep this manageable, self-services can be used. For example, users can register devices themselves. The required integrated solution needs a strong IT, Security and Compliancy Management environment, supported by the correct tooling.

Take the device's life cycle into account

Even though devices have their limitations compared to "normal" computers, IAM best practices can still be applied. The life cycle of a device can be taken as a starting point. After its initial registration, as part of asset management, the device is known within the organization. However, a device may also be used elsewhere or by another owner. Finally, at the end of the life cycle, access to the device's identity must be removed and all data on the device erased.

Use an IoT security framework

Furthermore, the use of an IoT security framework is recommended. Such a framework saves time and provides solid device security. Such frameworks also provide support for automation, which is relevant when using large numbers of devices. A framework must be tailored to the devices' specific use within the organization.

Be prepared for incidents

Finally, measures should be taken in case of an incident. An incident must be detected in time, which requires good monitoring in combination with advanced analysis. If monitoring already takes place in a Security Operations Center (SOC), this can be extended to devices. When a disruption is detected, for example, depending on its impact, access to specific devices or a complete set of devices can be (temporarily) denied. It is important to have a plan in place to deal with such unforeseen events and then return to normal business.

Protect devices with IAM

With the growing active number of devices connected to the internet within companies, the importance of applying IAM effectively is also growing. IAM is a proven mechanism for accessing data. This article describes the key challenges and measures that are specifically required for IAM devices. Awareness is therefore a prerequisite.

About the authors

Ton Slewe MBA CISSP is a Principal Consultant at Capgemini. He focuses on cybersecurity issues within public and private organizations. Christiaan Eenink B ICT is a consultant at Capgemini. He focuses on Identity & Access Management (IAM) processes and the connection with IAM technology within large organizations. MSc. Rob van Gansewinkel CISSP CISA SCF is a security architect at Capgemini. He focuses on supporting companies in enhancing their cybersecurity organization, processes and technology. MSc. Peter Seelen CISSP CCSP is a security architect at Capgemini. He helps organizations to set up their security, focusing on Identity & Access Management (IAM) and Cloud Security.




For more information, please contact the authors at:
ton.slewe@capgemini.com, www.linkedin.com/in/tonslewe, christiaan.eenink@capgemini.com, www.linkedin.com/in/christiaaneenink, rob.van.gansewinkel@capgemini.com, www.linkedin.com/in/rob-van-gansewinkel-6916a129 and peter.seelen@capgemini.com, www.linkedin.com/in/peterseelen

What do social media tell us about threats?

How can the police use social media analysis to predict and prevent incidents?

Highlights

- Many incidents, riots or attacks are directly or indirectly announced via social media
- Assessing the veracity of online threats can be automated
- In addition to active monitoring, social media will often have to be monitored passively in the future

On November 28, 2016, a man in Ohio drives into pedestrians, after which he attacks a number of people with a butcher's knife. Eleven people are injured, one of them severely. A few moments before his act, the attacker placed a threatening post on Facebook, announcing his intent.

Never before has so much information been shared on social media. Not only innocent people post messages, but football hooligans, terrorists and political activists also use social media channels. In the forecasting and prevention of incidents, unrest, riots or attacks, the police are already conducting social media analyses. But much progress can be made when this happens in a more focused, consistent and automated way.
In the analysis of social media, careful consideration must be given to the reliability of information and its risk assessment. In addition, it is always necessary to estimate the probability that a threat shared online will actually be carried out, as well as its impact on society. Research conducted by Kantar TNS, commissioned by Capgemini and Capgemini Consulting, shows that the absolute majority of Dutch people think that the government should make more use of social media to detect crime. The importance of their use in enforcement is high. They also contribute to increasing benefits and reducing costs because they are properly monitored by the government. The core of enforcement is that the government encourages or enforces compliance with the terms of service. This completes the circle of compliance, bringing together the components of service and enforcement. The vision from the circle of compliance is to connect the elements of prevention (information and service) and repression (control and sanction). This combination provides the best results and clear guidance for policy makers to achieve an integrated enforcement process, in which service and supervision complement rather than frustrate each other.

Figure 1: The absolute majority believes that the government should make more use of social media in detecting crime.

Police officers are placed in a difficult position when making a decision on whether to take a threat seriously or not and respond with a simple message on the specific social media channel. Every day, thousands of threats are posted on social media. Of these, the vast majority are not serious enough to investigate. Dealing with inaccurate information on social media obviously takes up a lot of police capacity. It is therefore becoming increasingly important for messages on social media to be quickly and thoroughly analyzed. The sooner the seriousness of an online message is clear, the faster the choice can be made to respond or not, and in what way. Currently, a distinction is made between collecting threatening messages, on the one hand, and on the other hand analyzing them. The analysis phase largely aims to determine the seriousness, context and background of the message.

What opportunities exist to monitor and analyze social media?

When it is clear whether a message needs to be taken seriously and whether further investigation is required, in most cases the first course of action is to attempt to find the source of the message. Because social media users usually send their messages under an alias, it is often not immediately clear who is behind a message. Next, the reliability of the source must be investigated. The fact that a source has a criminal past and therefore has to be taken seriously can, for example, be apparent from information provided by police systems.

By analyzing the social media, itself, it is possible to estimate the likelihood that the source of a specific message will translate their words into actions. For example, a source may have previously expressed similar threats on social media. In addition, the source's online network can lead to reassurance or additional concern. For example, when someone calls for a riot at a football match, but no one in his network belongs to the hard core of a football club, his call will be taken less seriously than when there are hardcore supporters in his network. In addition, the extent to which the message is forwarded or "liked" is an important indicator of potential turmoil.

Lastly, the number of online messages with (partially) the same content circulating on online media at the same time is also monitored. For obvious reasons, a message has more weight when it is placed by multiple users, or when multiple users make the same call to action (possibly using other words). If the information collected through social media has been analyzed and enriched with other messages, the next step is to use the decision-making information to counteract potential threats as soon as possible[1].

To ensure a quick response time (it may be a matter of minutes between reporting an upcoming attack and actually carrying it out), it is very important that continuous preventive monitoring of social media takes place. There is too little time to first manually check the veracity of all messages that can be classified as threatening, and then carry out another analysis. Therefore, the hope lies with software that can automatically tell the difference between a genuine threat and a "hoax", without the need for a police officer to act. This system could indicate a "red flag" when a message is so serious that action must be taken.

How do security services use the possibilities?

Social media analyses are often made in response to a phenomenon or rumor. For example, in the build-up to a high-risk match, various networking sites are monitored with the aim of gaining insight into where and when organized riots will take place. In large-scale situations, such as crises or events, social media monitoring is now a fixed component. In addition, to predict unexpected events (such as attacks or riots), continuous monitoring takes place from the police's Open Source Intelligence discipline. Various tools assist the police but, currently, monitoring and analyzing social media is still largely manual work. Specific searches must be implemented to allow the tools to do their work. This is a continuous process that is not completely watertight. Indeed, an important bottleneck of keyword searches is that not everything can be included. Examples are new (foreign) trending words among young people. These are not always familiar to the system user. Finally, at a certain time it must be determined that enough information has been collected, while it is unclear how strong the information position is at that time.

The Ministry of Security and Justice and its chain partners have been using the Coosto tool for several years, to gain insight into the subject of a message and the sentiment expressed by (and information on) its poster on social media. This active method of social media analysis starts with the formulation of a search. Social media are scanned on the basis of a specific topic, word or combination of words, such as "attack" or "football riot". The result of this query is a set of messages that match the query and fall within a specified period. This method is mainly used for enforcement during events. Its main aim is to unearth whether trouble is brewing.

As well as active monitoring, developments are also underway that make passive monitoring possible. A threat monitor has been developed for passive monitoring of social media. This tool automatically analyzes the content of messages with a particular topic and independently recognizes a threat level. The tool is designed to recognize and monitor individual messages, and makes quick intervention possible. This is necessary, as it may only be a matter of minutes between the time a message is posted and the moment that the words are turned into actions. Following social media closely and in real time makes it possible for the police to take adequate and proactive action[2].

What are the shortcomings of the current working method?

The flow of messages through social media is huge and will only grow. This represents an enormous challenge to the police in their efficient and effective handling of the data, performing analyses and strengthening their intelligence

position. In addition to determining the reliability of information, accountability also plays a role. The police must be able to justify in retrospect why an action or no action was taken. Continuing the current (mostly non-automated) method of information retrieval also requires an inordinate amount of human resources. In the security chain, ever-increasing quantities of information must be quickly processed into useful knowledge. Often the message flow for a particular subject is so large that only fully automated monitoring is effective.

It is also notable that current monitoring is still mainly active and reactive. Intelligence is mostly used for investigations in support of street patrol officers or to solve crimes. The fact that the proactive approach is still underexposed is evidenced by the objectives of the police intelligence teams OSINT (Open Source Intelligence) and RTIC (Real-Time Intelligence Center). Because whereas OSINT focuses primarily on detecting criminal offenses committed in the virtual world, the RTIC teams focus mainly on real-time support of colleagues on the street[3].

How can current processes be improved?

The proactive passive approach to social media monitoring will require greater attention in the future. The techniques that enable computerized monitoring of social media are constantly being further developed. Through the use of complex algorithms, in the near future they will be able to fully automatically expose terrorist networks, predict attacks, and signal when and where organized football riots will take place. It is too inefficient to manually analyze every threatening message on social media. That is also not the method currently being used, but more automation is needed to enable efficient and constant monitoring of social media and for analysts to work on those notifications that are considered serious by the system.

About the authors

Sjoerd van Veen MSc is a management expert and senior consultant at Capgemini. Thomas van het Ende MSc is a management expert and consultant at Capgemini. Both are active in the field of public order and security, and have a keen interest in intelligence issues and technological developments.

For more information, please contact the authors:
sjoerd.van.veen@capgemini.com, www.linkedin.com/in/sjoerd-van-veen-81622a30 and thomas.vanhet.ende@capgemini.com, www.linkedin.com/in/thomasvanhetende

[1]Monitoring and analysis information on social and online media, 2016, Gorissen & Johannink.
[2]Application of Social Media Data Analytics for the Ministry of Security and Justice, 2016, Bakker, Tops & Nonahal.
[3]Social media: factors affecting unrest situations, Johannink, Gorissen & Van As.

Cybersecurity and SMEs: in practice

How vulnerable is the backbone of the connected

Highlights

- SME dependence on third parties for ICT servicing is an important and urgent issue
- Our society is highly dependent on SMEs
- In cooperation with Interpolis, Capgemini Consulting Netherlands has developed a CyberPreventionService for SMEs, along the classic three-dimensional lines of Organization, People & resources and Technology
- In particular, the "organization" dimension is not sufficiently developed in SMEs
- The "technology" dimension is less of a blind spot, because third parties are usually deployed to take care of this

The increasing connectivity of the Netherlands provides many economic benefits. Nowhere in the Netherlands is digitization as prevalent as in the SME (Small and Medium-sized Enterprises) sector. But digital transformation should also include digital security. So, what is the state of cybersecurity within SMEs? There is little factual knowledge about cybersecurity in SMEs. By performing several dozen cybersecurity scans on these organizations, Capgemini and Interpolis have gained this knowledge. These scans (the so-called CyberPreventionService) show that policies, in general, need to be improved and that regular penetration tests (pentests) are absolutely essential to knowing how resilient SMEs are to digital threats and whether service providers and suppliers are delivering on expectations.

The role of SMEs in relation to cybersecurity is traditionally underexposed. There has been little research into the security of systems used by SMEs, which constitute 90% of companies in the Netherlands and largely determine economic activity[1]. Therefore, it is essential that greater attention is paid to the (digital) security of these organizations.

At the national level, the importance of cybersecurity in SMEs has been underlined for some time. The Cyber security Assessment Netherlands 2016 states that "SMEs take relatively few measures in the field of cybersecurity[2], compared to larger companies". This makes the backbone of the Dutch economy vulnerable. But how vulnerable?

Since 2014, consultants at Capgemini Consulting, in cooperation with insurer Interpolis, have set up the CyberPreventionService[3]. SMEs are assessed in eight different core areas. These eight areas are: policy and management, security information, awareness and training, laws and regulations, processes, physical security, access to company network, and internet/web. In addition, the technical state of the networks is tested by means of a technical scan (a so-called "pentest").

The connected society manifests itself most clearly in citizens and companies increasingly developing their activities online and expecting this to be safe. Again and again it has been shown that the cybersecurity of Dutch companies (from multinationals to the local baker) depends on safe connections.

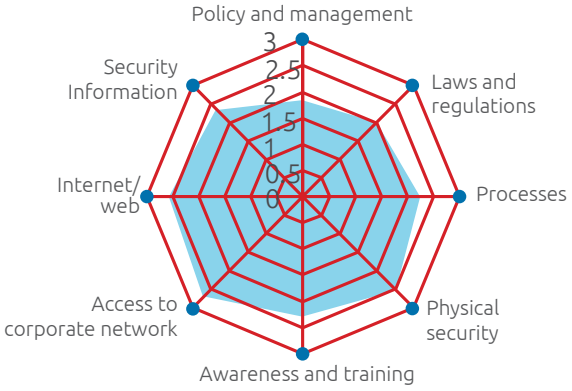
In 2015, Interpolis and Capgemini Consulting conducted research into "Cybersecurity in SMEs[4]" to find out more about the current state of cybersecurity in small and medium-sized enterprises. This research shows that about half of the companies surveyed use digital payment methods, such as credit card payments or online payment options. Also, about half of these companies use intellectual property and/or confidential data. Thirty-two percent of SMEs expect their business risk, in terms of cybersecurity, to increase over the next five years. In particular, the target groups of business services, retail and industry are emerging as sectors that see greater risks at the digital level.

Based on this research, Capgemini Consulting and Interpolis have intensified and rolled out the CyberPreventionService. The approach developed focuses on concrete recommendations along the classic three-dimensional lines of organization, people & resources and technology ("people, process & technology"). These dimensions were elaborated into eight core areas and were executed in five pilots with entrepreneurs. The three dimensions are central to the interviews and information collection. The results will be analyzed further and the recommendations linked to the so-called "gaps" found during the analysis.

Over the past two years, the CyberPreventionService has been performed several dozens of times. This makes it possible to carry out an initial exploration of the results. For this purpose, a special benchmark has been developed, which provides insight into the participating entrepreneurs' resilience and allows a comparison at sector level for some sectors. For example, an individual entrepreneur can see how their own company scores compared to the average of the participating entrepreneurs, and often their competitors.

The companies included in the benchmark can be categorized under the following sectors: retail, government, finance, industry, services and hospitality/entertainment. Possible answers to the questions were: whether certain measures have been implemented in an ad hoc way, partly, fully or not at all. With corresponding scores of 0-3. A score of 2 (partly) is, in our opinion, the desired baseline for cybersecurity.

Figure 1: Cybersecurity Benchmark



Source: Outcomes Cyber Security Benchmark, N = 26.

[1]https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf
[2]https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-2016/1/CSBN2016.pdf
[3]https://mijn.interpolis.nl/zakelijk/preventiediensten/paginas/cyberpreventiedienst.aspx
[4]https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf

In general, the results show that the companies score above the stated baseline. Especially in the areas of physical security, access to the corporate network and security of the website, the surveyed parties score adequately. Companies ensure that ICT facilities and information sources are properly physically shielded from unauthorized access, for instance by a closed door. Access to the corporate network is shielded by protecting the WiFi-network with a password, for example, and thoroughly shielding the host network from the regular network. Participating companies often invest in their digital environment by employing an external party to manage and maintain their network, digital services and workplaces, through which external expertise is gained. This also creates a risk: cyber risk could disappear from the agenda, as it is technically invested elsewhere.

However, when organizing business processes, a clear management vision is often lacking, as well as priorities and (internal) communication about this vision (core area "policy and management"). Because the urgency of the subject is lost, the "awareness and training" of staff is also a weak spot, which is only recognized if an internal incident or a major scandal occurs. Several companies that participated in the CyberPreventionService also found that they afforded too little attention to compliance with laws and regulations concerning cybersecurity and privacy. Since 2016, all Dutch organizations must comply with the Meldplicht Datalekken (duty to report data leakages) and must set up a procedure for this. Virtually no assessed company currently has such a procedure in place. Companies, in general, also score badly on specific or other legal requirements with which information processing in the organization must comply.

In addition to the controlled survey, a pentest has been performed by almost every participating organization. Most organizations have a number of critical vulnerabilities, including outdated versions of operating systems. Although this is not directly part of the presented benchmark, this recurring phenomenon underscores the need for a regular scan of the digital environment.

Conclusion

The practice of cybersecurity in SMEs in the Netherlands shows that much can be improved. The NCSCs statement that "SMEs take relatively few measures in the field of cybersecurity" can be interpreted as follows: technical measures are often taken but they are not tested and there is little activity at an organizational level.

SMEs are increasingly developing online activities and often rely on external service providers to take care of the technical aspects. Activities concerning physical security, access to the corporate network and the security of the website are often outsourced and, therefore, "dealt with" on paper. However, regular testing of the state of these security measures is often a blind spot.

In five of the eight core areas (policy and management, security information, awareness and training, laws and regulations, and processes) SMEs can make a big difference by bringing their (digital) security to a higher maturity level.

An approach that focuses on the greatest risks, based on insight into where the interests of the organization lie, is crucial to taking the right measures. Knowing where the leaks are located is essential to sealing them off. Organizations often have a blind spot for their weaknesses, because they think they have dealt with their risks by outsourcing them.

About the authors

Dana Tiggelman Ph.D. and Melle van den Berg MSc are security consultants at Capgemini Consulting. Melle specializes in cybersecurity and crisis management and was the lead author of the research paper SMEs and Cybersecurity from 2015. Dana specializes in cybersecurity and intelligence. Tim Wells MSc is a security analyst at Schiphol Group. He is concerned with the operational safety of all processes within the terminals and the innovation of security. Margot Hol MSc is a business consultant at Interpolis and develops prevention services.




For more information, please contact the authors:
dana.tiggelman@capgemini.com, www.linkedin.com/in/danatiggman and Melle.vanden.berg@capgemini.com, www.linkedin.com/in/mellevdberg, @mellevdberg, tim.wells@schiphol.nl www.linkedin.com/in/timwells90,Margot.hol@achmea.nl www.linkedin.com/in/margot-hol-977969115

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.nl** end **www.capgeminiconsulting.nl**

Identity crisis: how to balance digital transformation and user security?

Capgemini and RSA research shows that organizations that want to innovate in digitalization by rapidly developing new online services often invest too little in adequate cybersecurity measures. This poses significant risks, especially for the way users have access. The results show that companies are now taking action to strengthen their existing security measures. Especially in the wake of serious security incidents, investments in Identity and Access Management (IAM) significantly increase.

https://www.capgemini.com/resources/identity-crisis-how-to-balance-digital-transformation-and-user-security/

World Quality Report 2016-2017

This eighth edition of the World Quality Report shows the impact of trends such as the Internet of Things (IoT), through which organizations via digital technologies are looking to disrupt quality assurance and testing at an increasingly rapid rate. These features are increasingly needed to transform into a business facilitator and to safeguard the customer value of digital transformation programs. The World Quality Report examines the current state of the art in quality assurance and software testing in different sectors and regions worldwide.

https://www.capgemini.nl /thought-leadership/world-quality-report-2016-17

Digital Transformation Review 9: The digital strategy imperative, a steady long-term vision with a viable performance

In the ninth edition of the Digital Transformation Review, we explore how organizations can create a sustainable and successful innovation strategy. The research in this edition is based on our global panel of industry leaders and academics.
In this edition, we focus on four key themes:
• Creating a bold and balanced digital strategy.
• Should you choose to become a platform?
• Doing your digital strategy: acquisition, greenfield or organic growth?
• Working with an ecosystem of startups.

https://www.capgemini.com/consulting-nl/bronnen/digital-transformation-review-deg9-het-digitale-strategie-imperatief-een-gestage-lange/

The Currency of Trust: Why banks & insurers must make customer data safer & more secure

Capgemini's Digital Transformation Institute conducted a survey of 7,600 consumers in France, Germany, India, the Netherlands, Spain, Sweden, the United Kingdom and the United States. The questions relate to the image that consumers have of privacy and data protection in the financial sector. Researchers also spoke with 183 senior data security and security experts from France, Germany, India, the United Kingdom and the United States who work for banks and insurers with global sales of over $ 500 million. This report provides an insight into how financial institutions can tackle issues such as cybersecurity and data usage.

https://www.capgemini.com/consulting/resources/data-privacy-and-cybersecurity-in-banking-and-insurance/

Rebooting IT infrastructure for the digital age

IT infrastructure is a core component of successful Digital Transformation. However, very few organizations are making sufficient investments to transform core IT infrastructure. Only 15% of IT budgets are allocated toward core IT transformation. That means, modernizing IT hardware, networks and data systems to prepare these assets for the demands of the digital age, has taken a backseat. It is only a matter of time before outdated IT systems fail to keep pace with modern digital demands.

https://www.capgemini.com/consulting/resources/rebooting-it-infrastructure/

Trends in Security

Trends in Security is an annual Capgemini vision report, which outlines the main digital developments in the field of public order and safety. Download the Trends in Security report or individual articles published in 2016 or before:

https://www.trendsinveiligheid.nl

Capgemini

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 2016 global revenues of EUR 12.5 billion.

Visit us at

www.capgemini.nl

For more details contact:

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

INV 1B-105.17 © Shutterstock photos

People matter, results count.