
CYBERSECURITY
TRENDS 2020
TECHNOLOGY IS GETTING SMARTER – ARE WE?

TABLE OF CONTENTS

INTRODUCTION

As devices are undeniably getting smarter all the time, the question arises: Are we keeping pace with technological progress in terms of being "smart" enough to derive maximum benefit from these devices without suffering repercussions?

The rise of smart devices, which until a few years ago seemed like nothing more than a hopeful vision of the future, has occurred so quickly that the technology has become part of our everyday lives almost without us noticing the change. The gradual but persistent integration of technology into objects we use all the time is likely to change and impact social customs in ways that are yet to reveal themselves.

Every year, in choosing topics for Trends, ESET experts decide which aspects of cybersecurity and privacy seem likely to present some of the key challenges for the coming year. Over the five chapters that make up this edition of Trends, we review various cybersecurity issues with implications for people, governments and companies, as well as general concepts like privacy, democracy, digital transformation, and much more.

In the first chapter, Tony Anscombe tackles the topic of the US presidential elections and the echoes of the repercussions that fake news and denouncements of foreign interference had on the 2016 elections. But the US is not the only country to have been through this and it is almost certain that in 2020 the topic will be a big issue again. With that in mind, it's worth taking another look at how (dis)information and fake news could play a role in upcoming democratic processes.

Jake Moore then addresses another widely talked-about issue in recent times – machine learning, which is often misrepresented as artificial intelligence. Machine learning is used to describe a range of technological developments, but in 2019 one of its applications gained particular relevance for the general public with the briefly popular FaceApp and the rapid improvements in deepfake techniques, which have been increasingly visible over the course of the year. What are the cybersecurity implications of machine learning? In addition to being used to detect cybersecurity threats, could it be abused to violate the security and privacy of individuals and organizations?

All these issues are intimately connected to user privacy. In her chapter, Lysa Myers looks at how attitudes have changed since the Cambridge Analytica scandal, the implementation of legislation at various levels, and the likely implications for companies and governments resulting from user disenchantment about data privacy.

The trend for all things "smart" has not only reached the objects people use every day, but has begun to take importance on a larger scale. There are now many examples of smart buildings around the world, and there are expectations that more and more cities will soon become the latest in the long line to incorporate smart technology. However, could this lead to new types of attacks combining the digital and physical realms? Is cybersecurity advanced enough to ensure that these implementations can be carried out without putting users, citizens, and organizations at risk? Cecilia Pastorino discusses these and other issues in her chapter.

This paradigm shift is perhaps most visible in the digital transformation processes currently being implemented by many companies around the world, challenging IT teams to keep pace with all the technological change taking place. Camilo Gutiérrez Amaya dives deep into this issue, looking at the likely challenges for the corporate world in the near future.

One of the best tools to be prepared for the future is to stay informed, so why not read this report to find out what we can expect to see in 2020 and over the next few years?

2020: THE FOG THICKENS

- Fake news
- Targeted disinformation and propaganda
- The voting process
- De-mist-ifying it all?

Tony Anscombe
ESET Global Security Evangelist

2020: The fog thickens

"20/20" refers to perfect vision, but 2020 might just be another blurry year for the democratic process. What may stand in the way of our making informed decisions supported by facts?

As we head into 2020, there is one prediction from this entire Trends report that is probably guaranteed: there will be claims of meddling and manipulation in election processes during the year.

These issues are complex and while it is easy to point the finger of suspicion that there was interference, it can be difficult to prove beyond reasonable doubt. The complexity begins due to there being several types of interference that can cause election results to be shepherded to a certain outcome or to not actually represent the vote cast by the electorate. When looking at online or cyber-issues, these range from fake news and voting machine rigging, all the way through to targeting parts of the swayable population with biased information.

The 2016 US presidential election was shrouded in post-election controversy with claims of fake news, interference from other nation-states and the potential hacking of the voting process itself. Further, there are claims that the Brexit referendum in the United Kingdom was biased due to meddling and that in South America disinformation spread through WhatsApp possibly affected the outcome of the Brazilian elections. How can we expect voters to have confidence in the democratic process when all this is clouding the outcome?

This chapter summarizes some of the methods we will undoubtedly see used by individuals, activist groups, nation-states and even cybercriminals in 2020 as they attempt to interfere with the world's democratic processes for their own gain, whatever that may be.

Fake news

The Collins Dictionary awarded this term *Word of the Year* in 2017. Its rise to fame was largely due to the 2016 US presidential election and the continual claims by candidates that articles appearing in the media and stories spreading on social networks were not factual. The *meaning of the term* is self-explanatory and refers to the sensationalism of false information being disseminated under the guise of news reporting.

In the wake of the election, Pew Research conducted a *survey* on perceptions about fake news. The outcome was startling, with 88% stating that Americans are greatly or somewhat confused about basic facts due to fake news.

Ofcom, the UK's media regulator, issued a *report* stating that half of UK adults receive news through social media sites, with 75% of these stating this includes Facebook as a source. This is despite the fact that social media were not rated as impartial, trustworthy or accurate. TV remained the most used, with 75% of adults polled listing it among their news sources, but the influence of social media should not be underestimated and is here to stay.

There are different types of fake news: for profit, for political gain, for crime, hoaxes, and viral pranks. The types may even be combined: creating a hoax that puts a political candidate in a bad light may create political gain, and with the "right" advertising being displayed around the fake news story it may also generate a nice profit. If the creators of such a campaign could be identified they are likely to have committed a crime, but identifying the source is not always possible.

In the run-up to the 2019 UK general election a research organization, Future Advocacy, and a UK artist, Bill Posters, created a fake *social media video* , or so-called "deepfake". The video shows the main candidates appearing to endorse each other for prime minister. This example of fake news was created in an attempt to demonstrate the difficulty in identifying real vs. fake and that democracy is potentially being undermined.

But this issue is not new. I frequently stand at the checkout of the local supermarket and read the cover headlines of the magazines: celebrities splitting up, the UK Royal Family all getting divorced, or aliens landing in the car park. The readers of such magazines hopefully know the stories are fake when they choose to purchase them, but when we switch to internet stories, which are spread quickly to much broader audiences, it's not so easy to tell the good from the bad.

Some social networks and search engine providers are responsibly attempting to combat the issue, under pressure from political and public outrage. For example, Twitter has recently *announced a ban* on all political advertisements about candidates, elections and hot policy issues ahead of the 2020 US presidential election. But, this is a complex topic and it has even been referred to as a freedom of speech infringement if someone is denied the ability to post or place ads with a certain viewpoint. In reality: as fake news spreads, then page impressions increase and advertising revenue is gained, and not all actors displaying ads on websites are responsible.

The issue is speed of dissemination of the disinformation – a story appearing in the next hour will spread quickly, especially if the creator promotes it and spreads it from multiple accounts and networks at the same time. The companies responsible for the platforms have innovated detection methods and built reporting mechanisms to, when possible, automatically detect, or to allow users to report, fake news. Relying on reporting, though, is a flawed solution. As the disinformation has already been spread, many users will likely not take the extra step to report it … and those who have already seen (and perhaps been influenced by) the disinformation are unlikely to become aware of its retraction.

As a cybersecurity professional, I consider fake news that damages democracy to be malicious – much like malware intrusions on your devices. There needs to be a more robust technological solution to stopping fake news from spreading when it first appears and killing it at the source. In the same way that zero-day exploits are detected by antimalware products. With the adoption of machine learning, some innovative solutions are likely to come to market that will detect and suppress or delete at least some fake news before the user has been subjected to it.

Education is also a longer-term solution to this issue, but the results are slower. In July 2019, the UK, government published new safety guidance for schools; part of this updated policy states that every child will learn about confirmation bias and online risks as a compulsory part of the curriculum. This will help to enable pupils to spot techniques used for persuasion and to identify fake news and risks, but it will take many years for an entire generation to understand what may be real or fake. (My colleague Jake Moore deals with the specter of deepfakes in *another chapter* of this report.) However, understanding what is real or fake will give the next generation confidence in the democratic electoral system. More governments are likely to take this proactive stance and add this to their education policies. If they don't, then they should.

Targeted disinformation and propaganda

The Cambridge Analytica abuse of personal data shocked the world but did not surprise those of us who have always said – "if you aren't paying for it, then you are the product"; for example, each Facebook user in the US and Canada *generates more than US$130* for the company every year. The scandal eventually broke when three news organizations combined resources to cause enough traction for anyone to notice – after more than two years.

Fast forward a little in the story, and Facebook was fined US$5 billion by the US Federal Trade Commission (FTC) for its part in the data breach. I am not sure we can really describe it as a breach, though, as documents now in the public domain show that Facebook knew what was going on – it was more an abuse of trust for financial gain. On the day the FTC fine was announced Facebook's share price went up – it's clear the market either expected the penalty to be harsher or it understood that the deal struck with the FTC is actually in Facebook's favor.

The weaponization of information, be it disinformation or propaganda, is set to continue and will take many different paths as the benefactors explore and adopt new methods to attack democracy or to make money. At the center of this invasive and stealthy issue is data mining, something we can't see and for many people is hard to comprehend. The data points available about individuals, given that the majority of people *overshare on social media*, are extensive. The ability to adjust and manipulate the message sent to an individual is driven by technology, unlocking the power to individualize the messages sent to millions of people, all at the click of a mouse.

The voting process

Whether the ballot is verifiable is not a new issue and relates to both pen-and-paper and electronic voting systems. In addition, it's an issue that's unlikely to be resolved anytime soon.

Many states in the US have spent millions of dollars to upgrade systems that will be used in the 2020 elections. One state, Pennsylvania, has benefited from *US$14.5 million to upgrade electoral systems*, but even the new systems may be vulnerable. This is because the underlying underlying operating system, Windows 7, which – unless a fee is paid – will no longer receive patches from Microsoft once this version of the operating system reaches its "end of life" in January 2020, 11 months prior to the 2020 US presidential election.

At the DEF CON 27 hacking conference in August 2019, there were real-time challenges to find *vulnerabilities in election systems*. One such experiment showed vulnerabilities in a ballot marking system. In this instance the attacker had unrestricted physical access and direct connection to the devices, which should never to be the case in the real world. I hope someone might notice an attacker taking a terminal apart and connecting wires to it. This does depend though on the devices being physically secured prior to and during the voting process, which, in some instances in previous elections has not been the case. This may also lose relevance if the devices remain standalone and are never connected to a public network. While there are many devices that theoretically could be vulnerable, it does not necessarily mean they can or will be exploited.

It's clear that technological solutions to both registration and voting will continue to have issues. We continually witness mass data breaches and system compromises in companies and government departments, so why would voting technology or processes be exempt from similar attacks? The good news is that the 2016 US presidential election heightened the awareness of possible vulnerabilities in the electoral systems being used, which directly resulted in budget assignment as well as in the understanding of the need for the systems to be secure by design.

De-mist-ifying it all?

For 2020, there will of course be numerous elections around the world and countless issues highlighted in their systems and processes, both technological and physical. The use of all the methods mentioned here is to be expected, but the question is: to what scale will they be used and will the interference change the outcome?

As voters and, hopefully, believers in democracy, we will pressure companies that distribute fake news and disinformation into detecting and ceasing the practice. However, large profits for allowing these practices, and lack of engagement by consumers, probably means that we will continue to see the flood of misinformation, be it mildly misleading or fantastically fabricated, keep flowing.

As with many questionable practices, such as the abuse of consumer privacy we have been subjected to over the last 10 years, without government intervention and either regulation or legislation we will continue to a point where this practice can no longer be tolerated. Don't expect this to be in the next 12 months, though.

ML VS. ML: CREATING SECURITY OR ATTACKING IT?

- Fooling the naked eye
- Fooling the algorithm
- Boon or bane?

Jake Moore
ESET Security Specialist

ML vs. ML: Creating security or attacking it?

Advances in machine learning have brought considerable benefits to cybersecurity defenders, but the potential of the technology isn't lost on those who are looking to co-opt it for unsavory ends.

Machine learning (ML) is, without a doubt, changing our lives. Increased computing power and the use of vast storehouses of data are rapidly enhancing our capabilities in multiple industries. Furthermore, if ML's distant cousin also known as true Artificial Intelligence (AI) takes off too and computers start "thinking for themselves", we're in for a wondrous future where a lot of what was once thought unimaginable could become possible. For now, though, self-sustainable AI still seems a long way off – whereas ML is making headway in one of the most exciting technological developments in history.

ML has also brought various *benefits to cyber-defenders*, including efficient scanning, faster detection, and improvements in the ability to spot anomalies. Indeed, some cybersecurity companies have been taking advantage of the technology for years in order to enhance the detection capabilities of their products.

However, what if ML is misused to attack us and the systems we have made? It isn't hard to see why, and how, *ML- or even AI-based malware* might offer new and unique attack vectors – more powerful than what we are currently used to. It's becoming clear, then, that ML will be an important component in the future battle.

The technology has been advancing by leaps and bounds in other applications, too. In this Trends chapter, then, we will zero in on two ways in which ML algorithms could be weaponized to inflict harm.

Fooling the naked eye

Surely you've seen one of the many convincing face-swapping videos that pop up, especially on social media. Such deepfakes – doctored videos, audios or images that are designed to replicate the look and sound of real humans – can seem bafflingly legitimate and even shocking. The deepfakes may often involve celebrities or public figures apparently engaging in unexpected behavior or saying something outrageous and not normally endorsed by them.

Deepfakes are increasing in quality at an impressive rate, as seen in videos such as *this one* where a generated Barack Obama is made to say something the real one didn't actually say. Moreover, when you take a look at *Bill Hader* being morphed effortlessly between Tom Cruise and Seth Rogan, it makes you realize that we may indeed have a huge problem on our hands unless this threat is addressed. As with anything on the internet, the future could lead to this technology being used to damage public figures by making them appear to say whatever the creator wants, to damage society, or even to manipulate elections around the world.

Are we ready for the real impact of deepfakes? With political scandals, pseudonudes and almost unimaginable scenarios involving fake videos, we may be staring blankly at the beginning of an epidemic where the line between truth and lie may be impossible to determine. What impact could deepfakes have on society? In the light of the whole Cambridge Analytica scandal, in which data scientists were able to transform surveys and Facebook social graph data into a political messaging weapon via psychographic profiling, it seems that deepfakes could speed up such transformations in influencing the public in elections. Will there come a point where we don't even trust our own eyes and ears?

After FaceApp was literally plastered all over our faces and the groans and laughs rapidly died out, one question arose about the quality of such "wizardry" – might it one day create videos of people without their knowledge?

You need lots of data (many photos, videos and voice recordings) even to make a short deepfake clip where the creator is in control of what is said. However, getting a significant amount of data on a non-public figure is quite a task in itself. But this is only thinking in a 2019 mindset, so what if we think next year or in a decade? Could it take just a short Instagram story or two for someone to produce a deepfake that is believed by the majority of your friends online? This is very likely to happen and there will be an app on our phones that will create such deepfakes naturally and effortlessly.

Over the next decade we will see some previously unimaginable fake videos appearing with public figures but in time, these will include people closer to home, such as our colleagues, our peers and our family members. No doubt porn sites will exploit celebrities in obscure ways but, furthermore, cybercriminals will most definitely use such technology with great success to spearphish victims. Deepfakes could very easily muddy the water between fact and fiction, which in turn could cause some of us to not trust anything – even when presented with what our senses are telling us to believe.

So, what can be done to prepare us for this threat? First, we need to better educate people that deepfakes exist. People will need to learn to treat even the most realistic videos they see with a dash of skepticism. Also, and although difficult, technology needs to develop better detection of deepfakes. Although ML is at the heart of creating them in the first place, there needs to be something to act as the antidote, being able to detect them without relying on human intuition alone. Further, social media platforms need to recognize and address the potential threat as early as possible, as this is where deepfake videos are most likely to spread and have a detrimental impact on society.

Fooling the algorithm

Facial recognition is becoming more prevalent in current technology while also attracting some negative press. The implementation of facial recognition might not be 100% accurate yet, but again, it is only 2019 and things can only get better, right?

US cities have *banned facial recognition* being used by law enforcement after it wrongly identified 26 people as criminals who were law-abiding citizens. In fact, *research* by the US Government Accountability Office found that FBI algorithms were inaccurate 14% of the time, as well as being more likely to misidentify people of color and women. Furthermore, Microsoft has recently *refused to install facial recognition technology* for a US police force, due to concerns about ML bias. This is where data have been input by humans, who tend to have various unintentional biases that influence the ML outcome.

There are arguments for facial recognition to be rolled out everywhere, with the millions of surveillance cameras already capturing our near-every move in public. For example, if you take facial recognition in its most basic form, it offers a way of collecting information on who has been where at a certain time. This is not a million miles away from a good police officer who can recognize the local criminal on his or her patch (I know some police officers who can do this – they have incredible memories). So if facial recognition can become close to 100% accurate, then it may be watching our every move soon.

But if law enforcement knows the whereabouts of known criminals and suspects, what about criminals using the software to their advantage or stealing huge databases of confidential location data? It could be possible that the databases of people's faces could be compromised, meaning verification techniques such as facial or voice recognition could be fooled, and therefore, multi-layered security could be bypassed.

Boon or bane?

Complex ML-powered attacks are coming and let's not forget that some attacks are currently unfathomable due to the scale of the power they will use, so they have the potential to be bigger than we can possibly anticipate. It is possible that ML could be weaponized by attackers, so we need to be ready for such attacks and be aware of how to combat them. ML-driven attacks will be able to learn what worked and what didn't work on the fly and then retrain themselves in order to bypass existing defenses. As defenders, we need to understand how these ML-powered attacks will be created, what their capabilities might be and jointly tackle these future cyberattacks.

PRIVACY SEA CHANGE

- Design for privacy and security
- Improve ad tech
- Legislative consequences for breaches of trust
- Improve authentication and verification
- Let's turn this ship around

Lysa Myers
ESET Senior Security Researcher

Privacy sea change

Trust in our shared digital environment hasn't had a good run lately, and more and more people are on edge about safeguarding their digital data. What has been done and, even more importantly, what remains to be done for the tide to turn?

There's a certain "rite of passage" that happens when you've been talking about security and privacy for a while: you will make predictions about what the threatscape will look like in the future, and enough time will have passed that you can check to see how accurate your predictions were.

Mostly this happens on the near-future scale, such as this Trends chapter itself. Sometimes it's on the scale of a decade or more. In my own experience with this phenomenon I've noticed a few themes, most of which revolve around gaining or losing trust in our shared online environment.

As I was deciding what to write for this chapter, I did an internet search for the phrase "year of privacy" plus a recent year, e.g. "year of privacy 2018". Headlines including this phrase can be a good indicator that the author thought a big change was coming in regards to public perceptions of privacy, either positive or negative. I think the first time I declared that about a year in review was in 2013, so I was curious how many times this had been declared. For every year from 2009 to 2015, those search terms returned more than a million results. After that, every year returned "only" eight-to-nine hundred thousand results.

Does this mean that 2016 was the year a lot of people collectively threw up their hands in disgust and abandoned all hopes of having control over their personal information? In some ways, this may have been the case; there seems to have been a certain sense of collective resignation. But it also seems as if we had reached a point where legislators and judges had started to catch up with the collective ire provoked by a constant barrage of privacy gaffes and breaches.

And that barrage has continued – in 2019 alone, we've seen quite a few *countries* and US states *pass or implement new or expanded breach notification laws*. We've also *several US states* states put forth data privacy legislation (though only in California has this legislation passed). Several notable fines have been levied on companies responsible for *recent data breaches* (though these are generally considered to have been merely slaps on the wrist). Executives from *breached companies* have had to testify before congressional hearings about these incidents.

Change has been slow, and arguably these efforts have not made much of a positive difference yet. The general consensus among much of the US population is that they feel they *cannot trust* companies to protect their data, and this is the case in *other countries* as well. This situation, along with rampant fraud and other malignant traffic, has created a *"low trust" environment* in which we're increasingly interconnected but feel increasingly unsafe. When we have to approach everything on the internet with paranoia and skepticism, people feel understandably reluctant to engage with it.

In security, we often say it's best practice to "trust but verify": in the situation we find ourselves now, distrust is rampant and verification methods are full of holes. Until we remedy this, the internet will continue to be a scary place for most people.

So, what do we need to do to get out of this omnipresent sense of distrust?

Design for privacy and security

One of the most important things that needs to be done to improve customer trust is to create technology products and services that are designed with security and privacy in mind from the outset. The International Association of Privacy Professionals (IAPP) has created a document outlining its recommendations for the principles of *Privacy by Design*.

Much of what is covered is what one might expect: earning trust through openness and transparency, enacting end-to-end security, creating policies that establish accountability for the business, and obtaining *truly informed and ongoing* consent from customers. But there is one more recommendation that is particularly notable, and which many people might find surprising: permitting full functionality while respecting privacy, in such a way that it benefits both the business and the user.

Because the current model for so much of the internet is to use customer data as a product to be sold, this particular recommendation may require some truly innovative, "out of the box" thinking. Businesses that manage to accomplish this feat are likely to have a significant advantage in the marketplace.

Improve ad tech

While we're on the subject of selling customer data, we should also discuss necessary improvements in advertising technology. In *one survey*, less than 20% of respondents found targeted ads to be ethical behavior. *Other surveys* found that in some cases targeted ads could actually backfire and cause less customer interaction.

Companies that use high-pressure sales tactics such as *scarcity and social proof* don't fare well either. A survey in the UK reported that almost half of respondents said this behavior would cause them to distrust the vendor. One third expressed a negative emotional reaction (such as disgust or contempt). And 40% reported that these tactics would make them want to do the opposite of whatever action was being suggested.

The more often we're bombarded with high-pressure sales tactics and creepy surveillance tactics, the more quickly their (very limited) effectiveness declines. So many marketers have overused these strategies that they are likely limiting opportunities for other businesses as well. We need more effective ways to market that are honest, transparent, and respectful of our potential customers.

Legislative consequences for breaches of trust

Public sentiment about the trustworthiness of technology companies is unlikely to improve until it feels more likely they stand to lose at least as much as their customers do when privacy incidents occur. Although recent privacy-violation fines in the US and UK are breaking records, they represent a tiny drop in the bucket relative to the income that large businesses make from our data. Until these fines approach maximums that comprise a greater *percentage of a company's income*, they will continue to be more of a deterrent to small companies rather than to the mega-corporations.

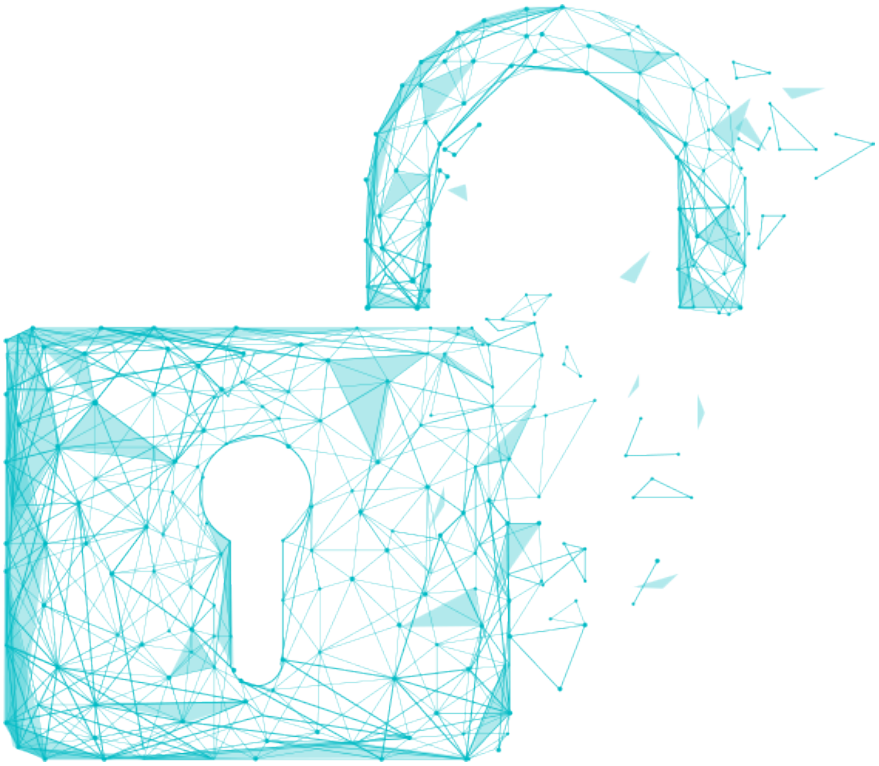
Improve authentication and verification

Usernames and passwords simply aren't enough to keep people's identities safe anymore. This can decrease trust both for online account holders as well as that of people interacting with potentially hijacked accounts. Multifactor authentication *significantly improves* this situation, but *very few people* have adopted it yet. To change this we'll need *improved education* about this technology, more companies *offering incentives* for using it, as well as continued improvements in its usability.

Let's turn this ship around

I was first asked to predict the state of security on the internet a decade hence, a little more than a decade ago. I said that I could see things going one of two ways: either we'd collectively wise up and things would be fine, or we'd continue to kick the can down the road and the internet would be an "unusable slag heap". While no one would successfully argue that people are using the internet less than they did ten years ago, we also have to wade through a whole lot more internet detritus now than we did in the 2000s.

Those old-timers among us who have been working in cybersecurity since the early days of the industry have been living in this state of distrust for decades; we saw the internet being built on shaky foundations that did little (if anything) to prevent misuse. Thankfully, we've also been thinking about – and talking about – what needs to be done to fix it. It's not too late to make meaningful moves to point privacy efforts back in the right direction. It is my hope that the appetite for necessary changes will continue to grow, so we can make those changes before my next decade in this business has elapsed.



SMART IS THE NEW SEXY: FROM IoT DEVICES TO SMART CITIES

4

- Smart buildings
- Smart cities
- Attacks on smart infrastructure
- Malware
- Identity and information theft
- Conclusion

Cecilia Pastorino
ESET Security Researcher

Smart is the new sexy: From IoT devices to smart cities

With more and more cities dripping with smart technology that changes the way municipalities manage their basic operations and services, what do these developments mean for the security side of things?

Since 1994, when the very first smartphone appeared, the word "smart" has come to describe any kind of device gaining enhanced functionality through software and usually an internet connection. Then, in 1999, computer scientist Kevin Ashton became the first person to use the expression "Internet of Things" (IoT). Ever since, expectations around the notion have been constantly rising. The 2010s have been notable for the revolution in the Internet of Things, and products such as watches, thermostats, lights, locks, cameras, toys, refrigerators, and other smart devices have now become a part of our smart homes, offices, buildings, and even cities.

Nowadays, the potential of IoT is not merely limited to the automation of tasks, but includes analytical processes that can be carried out on the vast quantities of information generated. Smart structures make use of a variety of interdependent technologies, such as machine learning, various wireless networking protocols, cloud computing, and IoT sensors and devices. The vast amount of information generated by networked sensors and devices is stored in huge databases and processed using machine learning and big-data analytics for the purposes of improving operational efficiency and developing a safe and productive environment. Thanks to these kinds of features, such systems have come to be described as "smart" – but smart does not always mean safe. While technology keeps taking huge leaps forward, some of us wonder when, finally, security will be incorporated into these changes right from the design stage.

Smart buildings

Smart buildings use technology to control a wide range of variables within their environments, with the aim of providing more comfort and contributing to the health and productivity of the people working or living in them. To do so, they use Building Automation Systems (BAS). Using hardware such as such as various kinds of sensors (light, temperature, air quality), cameras, access controls, etc., a BAS is able to analyze, predict, run diagnostics, and maintain various environmental conditions, as well as automate processes and monitor many variables in real time. Examples include optimizing power consumption for room temperature and lighting control, and automatic monitoring of security camera systems, elevators and parking facilities, among others.

The benefits of deploying smart devices are manifold. For instance, as *ESET Global Security Evangelist Tony Anscombe relates*, a well-known hotel in Las Vegas that automated A/C to operate only when rooms are occupied saved a cool US$2 million in the first year after the system was installed. According to the *Smart Buildings Market 2019-2024* report, in countries such as the US, the smart buildings market – including warehouses, factories, office buildings, and other corporate, industrial, and government structures – is estimated to grow 16.6% by 2020 compared to 2014. As such, more than 80% of today's new buildings incorporate at least an element of IoT and technologies related to the smart buildings market.

Smart cities

In 2019, *CES* included an entire area devoted to smart city initiatives currently under implementation (or in planning) around the world. Some of them are aimed at improving transportation by using sensors to evaluate traffic flows, and then controlling traffic signals on the basis of these measurements. Others are for automating lighting through light sensors, measuring temperatures, incorporating monitoring systems consisting of networks of cameras and many other sensors to gather information that is then analyzed at a monitoring station in order to gain insights into everything going on in the city. Just as in smart buildings, but on a larger scale, it all revolves around sensors that gather information and where machine learning is used to analyze the data in order to efficiently automate a related service.

The problem is that many of these cities are not fully prepared to safely manage the large volumes of information produced by these systems, and an attacker could easily gain access to sensors, adjust measurements, and make changes to services used in transportation, traffic, lighting, or other critical infrastructure. We have already seen proofs of concept of different types of attacks on smart cities and *automated systems* at conferences such as *Black Hat* and DEF CON. Furthermore, if cities such as Atlanta, whose *goal is to become a world-leading smart city*, have not managed to avoid threats that exist already, such as *ransomware*, what reason do we have to believe that they can tackle even larger threats? Experts have expressed concerns that smart cities are experiencing rapid growth but our ability to make them secure *is not keeping up*.

Attacks on smart infrastructure

On the one hand, it would appear that attacks on smart buildings and cities could only be carried out using detailed plans in which cybercriminals aim at a specific target. On the other hand, many BAS systems, as well as the sensors and devices used in smart cities, are directly exposed to the internet. Currently, searches on tools such as Shodan and Censys return results of more than 35,000 BAS systems, as well as hundreds of thousands of critical devices within public reach on the internet.

Many of these devices and systems do not have sufficiently strong authentication systems, have no kind of protection against brute-force attacks, are not updated, are not protected by any kind of security solution, or simply have unsecured setups that could allow an attacker to take control of the equipment.

Malware

Although the systems used by smart buildings and cities do not browse the web or open email, they still need to protect themselves against malware, which could give a cybercriminal access to critical information or cause damage to hardware. Malicious code can be propagated through the web access interface used to administer IoT devices, vulnerabilities in systems and even through physical access to USB ports that are unprotected or within the reach of anyone passing by. It is also important not to neglect protection of the network, especially in places where users will plug in personal devices, which could be compromised.

The systems used by smart buildings and cities could be attacked, for example, via *botnets* that take aim at smart devices. Is it far-fetched to imagine that, in the not-too-distant future, the IoT resources of an entire city could be hijacked by an attacker to generate millions of dollars through cryptocurrency mining? And cryptojacking is not the only threat. Three years ago in *Trends 2017: Security held ransom* we presented the concept of jackware to describe malware that tries to take control of a device whose primary purpose is neither data processing nor digital communication. And immediately we derived from that the concept of *Ransomware of Things*, which refers to malware capable of blocking access to smart devices. That year, *we discussed a proof of concept* involving the remote hacking of a moving car.

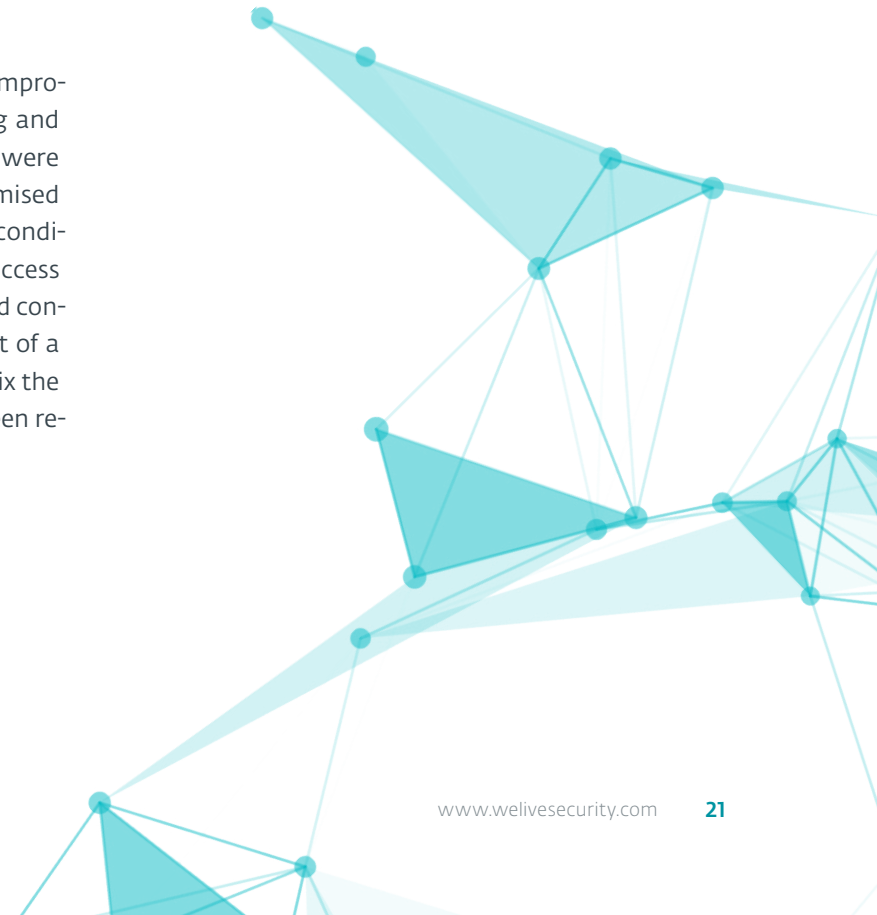
What would happen if an attacker managed to compromise the automation system of a smart building and threatened to cause havoc unless a ransom fee were paid? The types of systems that could be compromised include critical elements such as heating and air conditioning, fire detection and extinguishing systems, access controls, lighting, and the building's command and control center. This scenario may sound like the plot of a science-fiction movie, but in fact incidents that mix the concept of ransomware with BAS have already been reported – and *we have dubbed it siegeware*.

Identity and information theft

Physical access to smart buildings tends to be controlled through IT systems whereby users identify themselves with biometric data or physical tokens. Such systems can be compromised through social engineering or shortcomings in their implementation, which could allow an unauthorized individual to gain physical access to restricted sectors.

Besides, digital identity theft can cause havoc if the attackers gain administrator privileges, which allow them to control the system(s) as they please. Once the attackers manage to make off with the victim's access credentials, they may go on to install malicious code, steal information, navigate through the system, and carry out any number of other damaging activities.

IoT sensors and devices used in most smart buildings and infrastructures can also act as an entry point to the network. This was the case for a casino that *fell victim to an attack* in which cybercriminals got into its network after exploiting a vulnerability in the smart thermostat of a fish tank in the lobby. They then accessed the casino's database, stealing information that included gamblers' personal data.



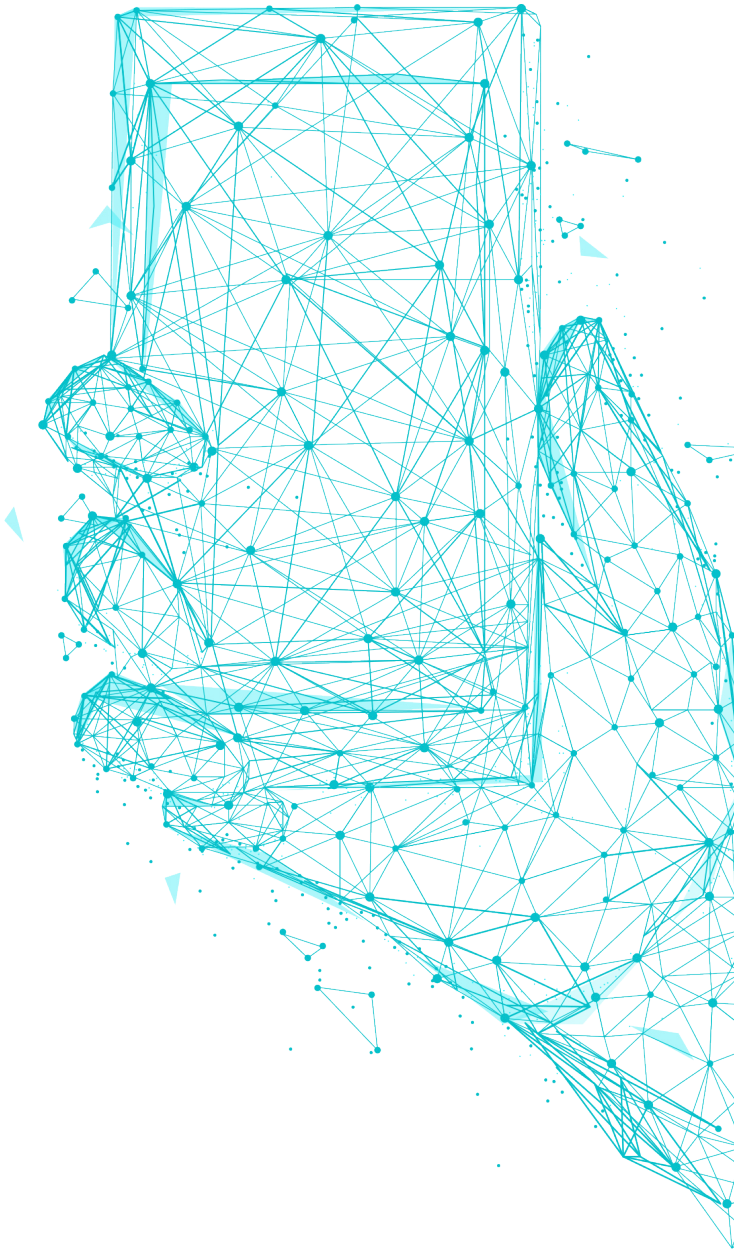
Conclusion

Smart buildings and cities are no longer the stuff of science fiction, but a reality of the world we inhabit. So far, the security incidents reported have been at an infrequent enough rate that they can be considered as isolated cases. Still, it is clear that control systems for buildings and cities have become targets for cybercriminals.

The security measures to be taken in order to tackle these new threats are the same steps we always emphasize with each new wave of technological evolution: allocate sufficient budget for security, buy from vendors that have baked in the security at the time of purchase, implement programs for handling vulnerabilities, keep systems up to date, monitor the network and devices, and make sure you have security tools and the support of partners with knowledge in the field of security.

Additionally, there is a clear need to support legislation to mandate security right from the design of smart devices, and this is something likely to arise in the coming years, especially in the light of recent *initiatives in the UK* and California. Just as standards exist to regulate critical equipment, it is time to start analyzing what security norms and measures should be minimum requirements for the smart devices that interact with our information and privacy.

Many of us already live in cities with multitudes of sensors and cameras connected to the internet. In a not-too-distant future we will spend a large part of our daily lives working and shopping in hyperconnected buildings packed with technology. And while all of this progress might seem exciting and impressive, we must not forget that behind it all, there have to be smart people.



SECURING THE DIGITAL TRANSFORMATION

- Changes in IT must be supported by changes in cybersecurity management
- Technological variety as a driver of change
- The road to mobility
- Concepts to retain in the digital transformation
- So, what should companies do?

Camilo Gutiérrez Amaya
ESET Senior Security Researcher

Securing the digital transformation

As organizations set out on, or continue down, the path of digital transformation, they have to rethink all aspects of their operations. How can they reap the benefits of going digital without getting derailed along the way as a result of a failure to address underlying cybersecurity challenges?

Due to market dynamics, digital transformation has become a fundamental issue that has an effect on all aspects of a company's affairs. The implementation of all these new technologies – a journey that many companies embarked on a few years back with the aim of delivering more value to their customers – requires cultural change at the organizational level. It is no wonder, then, that this represents a major challenge for all involved businesses.

Naturally, information security should not be seen as something separate from these efforts. Rather, it as an important part of the goals that companies need to plan for in order to avoid being left behind in the race due to lapses in cybersecurity.

Digital transformation tends to involve rethinking the processes and strategies of each individual company and, in so doing, allowing each to benefit from digital technology. On the other hand, this leads to new risks – and companies must not lose sight of these perils.

Changes in IT must be supported by changes in cybersecurity management

Companies that are already undergoing changes that are part of their digital transformation have discovered that they are exposed to the development of business models that include a large technological component, and as a result, their IT teams have had to adjust in order to support the speed of this change.

All this change means that, little by little, companies are moving from having the majority of their resources centralized to having to adopt a wide range of new services and assets in order to support their day-to-day activities, leading to an increase in the variety of technologies and platforms they need to monitor.

This difficult process of transformation – which, according to a survey by *McKinsey*, eight in ten organizations have decided to undertake over the last five years – has had direct implications for the organizations' cybersecurity posture. Companies need to work actively towards reducing the chances of falling victim to a cyberattack or data breach. As a result, management teams have found themselves immersed in new paradigms that allow them to fulfill this mission – but without impacting their normal business operations. In order to operate successfully in a digital ecosystem, organizations need to be able to secure their data during the transformation process.

According to a *study* that the Ponemon Institute carried out in a number of countries in 2018, 72% of IT security professionals believe that a sense of urgency around achieving digital transformation increases the risk of a data breach. When coupled with the fact that 45% of organizations said that they do not have a strategy for dealing with the digital transformation, this is grounds for concern, to say the least.

It is vital for security teams to have a constant flow of information about all the changes going on inside their organizations. For this reason, smart technologies, including threat monitoring, are important to provide a base on which other processes can be run securely, maintaining compliance with standards across the entire organization.

Technological variety as a driver of change

Companies need to see information security as a part of the digitalization process. As multiple technologies are now available for this process – including *cloud computing*, mobile platforms, 5G connectivity and machine learning, to name just a few – it is important to understand that no single technology or application is going to be enough to guarantee data security and business continuity.

One of the main hurdles for companies that are embarking on the journey may be where to start. In fact, the starting point is understanding that all of this transformation is also radically and rapidly changing society as a whole – the way we work, socialize, buy things, and interact in the many aspects of our daily lives.

Concepts to retain in the digital transformation

Beyond these specific technologies, which in any case will keep evolving, we must not lose sight of key concepts like privacy. We are living in a time when new, stricter *laws on personal data protection* are continually being adopted. As a result, people are gradually becoming more aware of their rights and are more concerned about how companies handle their data.

Over the coming months we will see organizations implement major changes in almost all areas of their businesses. The common thread running through all this will be how they handle information and the data involved in their operations. Therefore, business models that generate client trust will be a differentiating factor.

The road to mobility

From all these scenarios for change inside companies, there is one in particular that will be a major factor in accelerating the process in 2020 – employee mobility. Undoubtedly, our ability to stay connected to networks, regardless of where we are, keeps increasing organizations' attack surfaces and exposure to risk.

All this change has been taking place slowly but surely over recent years, but companies' ever-increasing speed of adoption of mobile technology often occurs without due consideration of security. This is why it's important for companies to stop thinking of security in the traditional way and instead consider adopting adaptive models that can respond to change.

And even more urgently, IT security teams need to dive head first into the use of monitoring technologies, because detection technologies alone are not enough. It is important for companies to develop processes for responding to incidents and then bring operations back to normal by resolving those incidents and applying suitable corrective measures.

So, what should companies do?

In terms of what companies are going to face over the next year, there are at least five key considerations they need to focus on in order to handle this transformation securely:

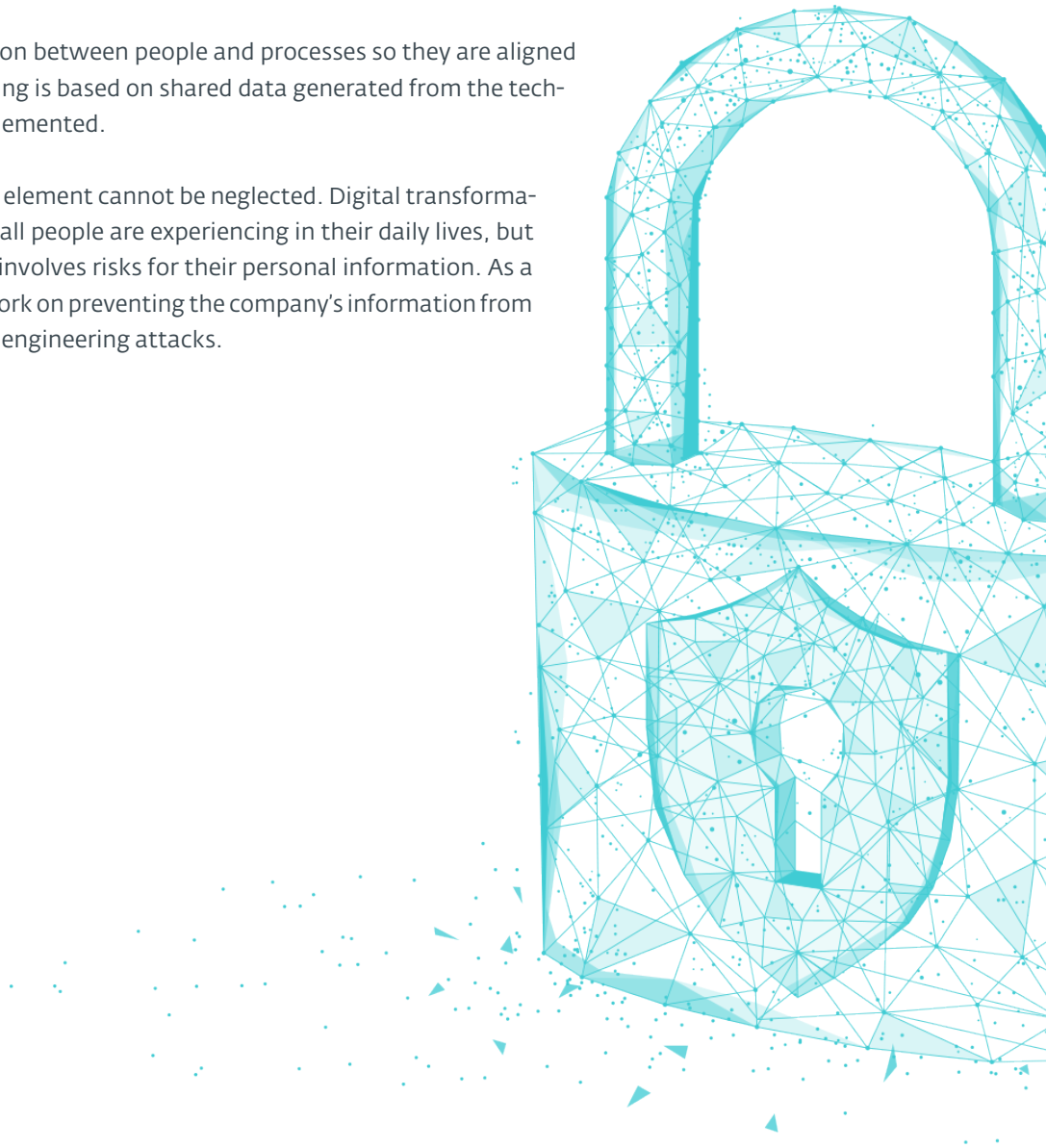
1. Find a balance between the implementation of new technology and cybersecurity. If they aren't balanced from the start and if security isn't seen as an enabler for the business, there are going to be more problems than solutions.

2. Develop projects that facilitate both the visibility and control of technologies. In doing so, the focus should not only be on preventing incidents, but should also consider detecting and responding to an incident.

3. Security can't be focused only on devices, because the quantity of equipment and technology is constantly growing, making it complicated to implement security on each component individually.

4. Foster greater collaboration between people and processes so they are aligned and so that decision-making is based on shared data generated from the technology that has been implemented.

5. And of course, the human element cannot be neglected. Digital transformation is something almost all people are experiencing in their daily lives, but often with behavior that involves risks for their personal information. As a result, it is important to work on preventing the company's information from being vulnerable to social engineering attacks.



CONCLUSION

The challenges to come are undoubtedly great, and we need to prepare ourselves, from the technological and educational perspectives alike. By doing so, both current and future generations will have better tools to tackle these challenges, and technology will be given the opportunity to realize its true potential, translating into a better quality of life for humanity.

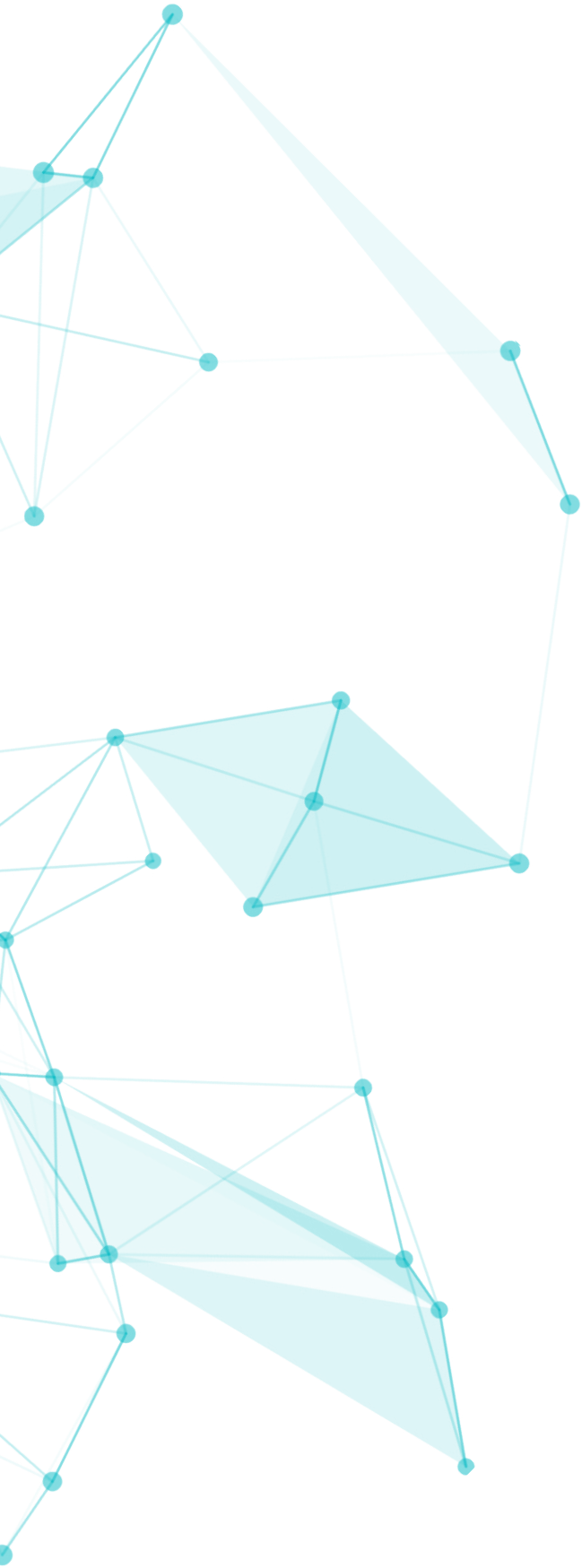
As this edition of Trends has made abundantly clear, our world is evidently set on continuing to evolve in its use of technology and becoming (even) "smarter" than it is at present. But only when advances in artificial intelligence have actually enabled machines to think for themselves, only when the transformation toward what we think of as smart cities has become a global phenomenon, and only when the process of digital transformation that many companies are currently undertaking has become past history, will we be able to analyze with more precision what the actual costs of this process were.

What is absolutely clear is that, considering the way things look at the moment, cybersecurity will continue to be viewed as an issue of secondary importance when it comes to technological development. This will have consequences in the short term.

On the one hand, there are encouraging signs that more and more people are coming to recognize the importance of cybersecurity, and the need for it to play more of a leading role as we head into the future. However, given that, in the last five years, eight in ten companies have started out on the path of digital transformation, coupled with the *growth in data breaches* on a global scale and the *predicted increase* in costs for companies to deal with them, it seems impossible to avoid these types of incidents.

Additionally, if we stop to think about the growth anticipated for the construction of smart buildings and cities, and of the fact that many cities that are currently invested in the concept of "smart" have fallen victim to known threats like ransomware, what reason do we have to be optimistic and believe that the future will be any better in terms of information security practice?

Similarly, if we take as points of reference the current advances in the beneficial use of machine learning, the phenomenon of fake news, and what we can expect from a still distant future in which artificial intelligence has been developed, the challenge of being prepared for what is to come could provide us with the opportunity to take measures that really give cybersecurity more of a leading role.



Deepfakes have already given us a sense of their potential impact, creating confusion and sowing uncertainty about which pieces of information are true and which are false. In turn, this spreads mistrust among individuals, who, by being more interconnected, continue to expose their data and personal information due to a lack of knowledge – or implementation – of basic security practices. Not only that, but many of these individuals have to vote in elections in countries that have opted for electronic voting, despite the evidence of problems with such systems.

Returning to the question we asked earlier, there have, in fact, been some positive signs that give us cause for optimism. Companies like Facebook, together with other big companies and universities, have demonstrated their willingness to fight against phenomena like deepfakes by launching initiatives such as the *Deepfake Detection Challenge (DFDC)*, which is intended to promote the development of new technology capable of fighting back against deepfakes.

Furthermore, recent times have seen changes to the legislative and regulatory landscape relating to data privacy. While these may have been slow to occur and have perhaps not yet generated a significant impact, they are at least developments in the right direction.

There is still a lot of work to do and governments still need to intervene and promote measures that provide a framework and a direction for the path forward. On the one hand, there is still a lack of awareness about many aspects of information security. On the other hand, the distrust displayed by many people in that their personal data is being appropriately protected reflect the fact that they are continually less shielded from the impact of cybersecurity and privacy on their lives. This may be an indication that, across the range of issues discussed in this Trends report, further consumer education about cybersecurity issues is an important factor for further consideration.


CYBERSECURITY
EXPERTS ON YOUR SIDE