ISO focus

#132

Your gateway to International Standards

The cyber **secrets**

ISOfocus January-February 2019 – ISSN 2226-1095

ISOfocus, the magazine of the International Organization for Standardization, is published six times a year. You can discover more content on our Website at **iso.org/isofocus**, or by staying connected with us on:

Head of Communication | Katie Bird
Editor-in-Chief | Elizabeth Gasiorowski-Denis
Writer | Barnaby Lewis
Contributing writers | Robert Bartram, Rick Gould
Copy editor and Proofreader | Vivienne Rojas
Designers | Xela Damond, Pierre Granier, Alexane Rosa
Translator | Alexandra Florent

Subscriptions and back issues

If you enjoy *ISOfocus*, you can download the pdf for free or subscribe to receive printed issues through our Website **iso.org/isofocus**. You can also contact our customer service at **customerservice@iso.org**.

Contributions

You can participate in creating this magazine. If you think your contribution can add value to any of our sections, please get in touch at **isofocus@iso.org**. Views expressed are those of the respective contributors and are not necessarily those of ISO or any of its members.

#132

Photo: Markus Spiske/Unsplash

ISO focus

January-February 2019

Photo: Kevin Ku/Unsplash

Photo: Hal Gatewood/Unsplash

Confidence
to continue delivering

***John Walter**, ISO President.*

As I finish my first year as ISO President, I feel great pride and a sincere sense of accomplishment. Looking back over this past year – in fact, over the last decade – it's remarkable how much ISO has achieved and how well it has performed. Such performance is not only focused on our strong standards development processes and deliverables, but also on the ways by which we've been able to provide assistance and guidance to many of our members around the world.

You've heard me say on a number of occasions that standards developers around the world are the best examples of friendship, cooperation, trust and collegial working relationships. We open doors and build bridges. We create and nurture trusted colleagues. We respect and value every person and every national standards body. We do not discriminate against any person, organization or nation. We welcome and accept all participants as they bring a sincere commitment to International Standards and to the use of those standards for the benefit of our global village. The world needs more ISO.

For this reason, we all have an obligation to maintain and grow ISO as a healthy and vibrant organization. The world expects nothing less of us. When I've met with industry and government leaders in every part of the world, I've been warmly welcomed. They are eagerly seeking solutions to serious and grave challenges. We often spend time describing and discussing the options presented by International Standards. At the end of such sessions, they've unanimously expressed their desire to work with ISO, to collaborate, to cooperate and to support. Such commitment on their part inspires me greatly and is one reason why Secretary-General Sergio Mujica and I continue to expand our fruitful discussions with the world's top leaders.

However, we must do more – we must reach out and engage ; we must continue to provide solutions. The future of this world may depend on us. Building value for our members has been key for both Sergio and me. I'm very pleased with the ways by which we've delivered on our commitments and the ways in which we've engaged with the global community. At the helm, Sergio speaks with knowledge, intelligence and authority on all parts of the organization and on every region of the world. We've received unwavering support from every ISO Council member, with increased involvement and engagement in our revised governance processes. Such an involvement can only benefit ISO.

Engagement with international organizations has been a crucial part of our work. Last year, as ISO President, I made a commitment to you that we would build stronger bridges with our sister organization, the International Electrotechnical Commission (IEC). I'm excited and immensely pleased to note the increased cooperation and collaboration between the two organizations. Much of that success is due to the energy and leadership of my long-time and trusted friend, IEC President Jim Shannon.

Looking ahead, we will need to increase our efforts to support the United Nations (UN) 2030 Agenda for Sustainable Development, designed to shift our world onto a more resilient and prosperous path. It's important that we use our time wisely and move forward as decisively and swiftly as we can. With just 11 years to go, our engagement with the UN needs to be stronger than ever and we will continue to invest extensively in helping the world achieve all 17 Sustainable Development Goals.

These efforts are only part of what we do – albeit an important part – to address the world's vast global challenges. I personally worry most about cybersecurity. It is without doubt one of the major concerns of the modern world. If disruptive and invidious cyber-activity is able to terminate or corrupt our global interconnections, all of our best processes and efforts will come to naught. Digital connectivity plays a pivotal role in unlocking innovation and prosperity for humankind. Yet increasing cyberthreats present a major stumbling block on our collective path to progress and governments and industry need to build capabilities in this area – very quickly.

Gone are the days when companies could pass the headaches of cybersecurity to the IT department. Those headaches have now become an issue of business sustainability and survival. International Standards are essential to ensure that cybersecurity programmes are rigorous and effective. As I've stated to government and industry leaders worldwide, ISO is uniquely positioned in this era of massive cyberspace transformation ; and we're building a first-rate portfolio of standards for organizations to embed in their daily business processes and products.

As we embark upon a new year, we're not at all certain what to anticipate regarding cybersecurity. What do cybercriminals have in store for us in 2019 ? What do we need to do to protect against them ? I hope that this issue of *ISOfocus* will go some way to answering those questions. In today's fragile cybersecurity reality, International Standards are more in demand than ever.

On a very personal note, I believe that every individual in the International Standards system has a moral obligation to set aside our differences, to heal over our petty disputes and to embrace globalization. Isolation and the building of walls between us will simply lead to massive institutional and environmental failure, and eventually disaster. As members of this international civilization, we can and we must cooperatively address the challenges that face this Earth. Does any one of you really want your children to inherit a planet that can't survive because of our self-interest and negligence ? ISO standards are now helping to address and resolve global challenges, and we must ensure that they continue to do so in the future. The stakes are too high for anything else. ■

A new change is in the air

QUOTE CARD **Bertrand Piccard**

What the leading figure behind Solar Impulse has to say about the role of standards in the world

#4thindustrialrevolution

To highlight the importance of standards for the Fourth Industrial Revolution, ISO ran a global campaign on its social media platforms from 12 to 26 October 2018. After launching with the celebration of World Standards Day, we focused on how ISO standards supporting the adoption of cyber-physical systems will benefit people's daily lives in areas such as health and safety, transport, personal data protection, and life sciences technology.

CAMPAIGN

The campaign brought together ISO members, stakeholders and industry experts to talk about the need to develop standards that will ensure the seamless adoption of emerging technologies in our everyday life

+3 300 000
IMPRESSIONS

4th In
ISO/TC 22/SC 31
Data communication
SOME INTERNATIONAL STANDARDS SUPPORTING THE 4TH INDUSTRIAL REVOLUTION

+500 CONTRIBUTORS
TO OUR CAMPAIGN

THINGLINK **International Standards and the Fourth Industrial Revolution**

Overview of some related ISO/TCs

VIDEO **Standards and artificial intelligence Part 1**

Interview of Wael William Diab, Chair of ISO/IEC JTC 1/SC 42

VIDEO **Standards and artificial intelligence Part 2**

Interview of Wael William Diab, Chair of ISO/IEC JTC 1/SC 42

+15 500
VIDEO VIEWS

+1 700 000
USERS REACHED

VIDEO **Standards and blockchain**

Interview of Philippa Ryan, ISO/TC 307/WG 3, *Smart contracts and their applications*

HOW TO TACKLE TODAY'S IT SECURITY RISKS

Photo : Kevin Ku/Unsplash

by Barnaby Lewis

Industry experts estimate that annual losses from cybercrime could rise to USD 2 trillion by next year [1]. With countless new targets added every day, especially mobile devices and connected "things", a joined-up approach is essential.

The attraction of cybercrime to criminal hackers is obvious: tangled webs of interactions, relatively low penalties, disjointed approaches on money laundering and potentially massive payouts. The key is preparation and seeing vulnerabilities, and resilience, in terms of interactions with overall management systems, and that's where information security management systems (ISMS) standard ISO/IEC 27001 comes in.

This is the flagship of the ISO/IEC 27000 family of standards, which was first published more than 20 years ago. Developed by ISO/IEC JTC 1, the joint technical committee of ISO and the International Electrotechnical Commission (IEC) created to provide a point of formal standardization in information technology, it has been constantly updated and expanded to include more than 40 International Standards covering everything from the creation of a shared vocabulary (ISO/IEC 27000), risk management (ISO/IEC 27005), cloud security (ISO/IEC 27017 and ISO/IEC 27018) to the forensic techniques used to analyse digital evidence and investigate incidents (ISO/IEC 27042 and ISO/IEC 27043 respectively).

These standards are not only about helping to manage information security but will also help to identify and bring criminals to justice. For example, ISO/IEC 27043 offers guidelines that describe processes and principles applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security, as well as any other digital investigation.

The key is preparation and seeing vulnerabilities.

Staying ahead of the game

Keeping this family applicable to the needs of businesses small and large through a process of constant evolution is a serious responsibility for ISO/IEC JTC 1's subcommittee SC 27 on IT security techniques. It's in large part thanks to the contribution of people like Prof. Edward Humphreys, who chairs the working group responsible for developing ISMS, that it remains one of the most effective risk management tools for fighting off the billions of attacks that occur each year [2], which likewise continue to evolve in their targeting and methods.

I spoke with Prof. Humphreys, a specialist in information security and risk management with more than 37 years of experience in consulting and academia. I began by asking him about the fundamentals of ISMS. Just how can they can keep ahead of the criminals to protect businesses and consumers?

[1] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", Forbes Online

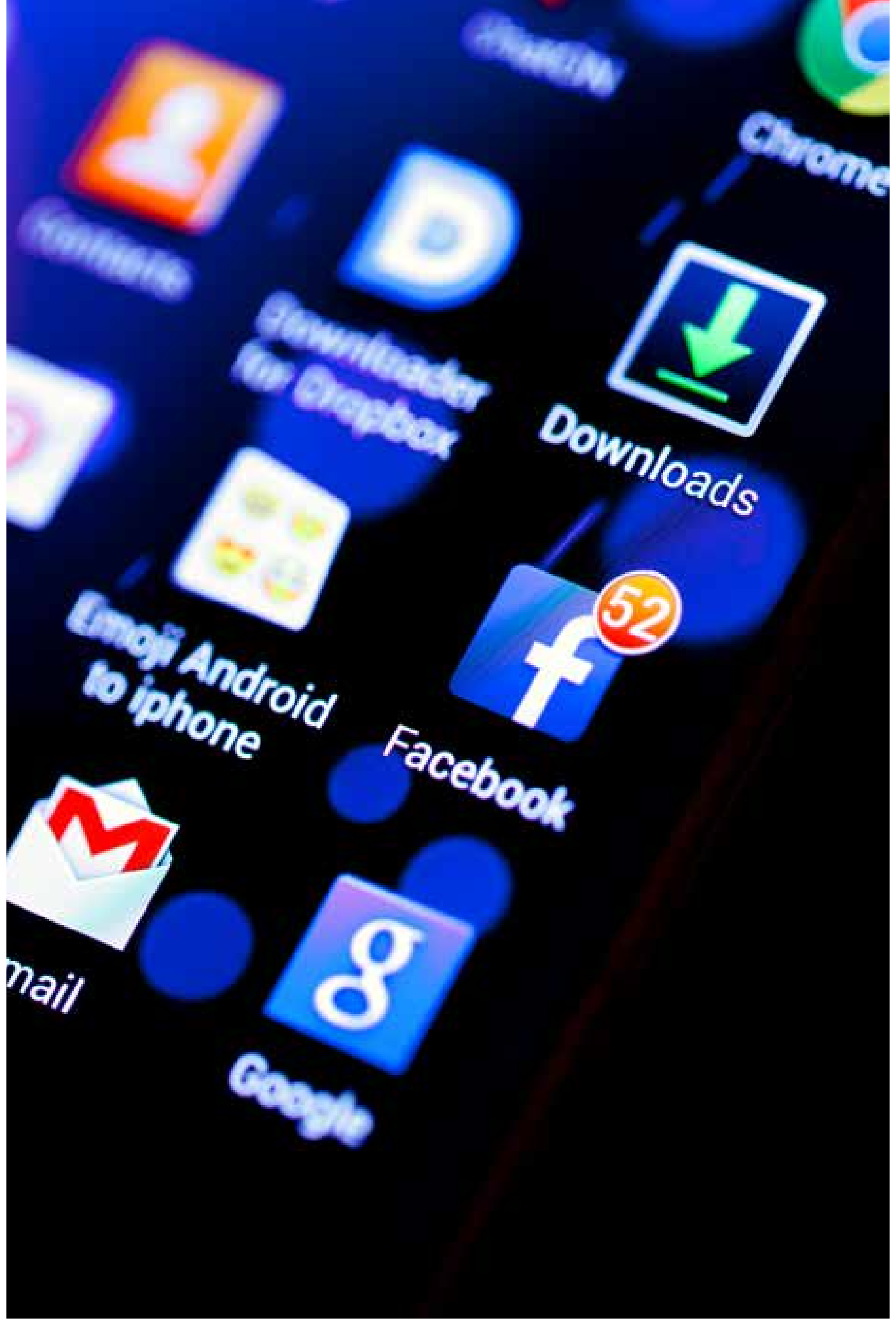
[2] "Internet Security Threat Report", Volume 23, Symantec, 2018

"It's true that risks that threaten information, business processes, applications and services are continually evolving. ISO/IEC 27001 is a continual improvement standard, which means the built-in risk management process allows businesses to keep up to date in their fight against cybercrime."

According to Prof. Humphreys, the continual improvement aspect of ISO/IEC 27001 means that an organization can assess its risks, implement controls to mitigate these, and then monitor and review its risks and controls, improving its protection as necessary. In that way, it's always on the ready and prepared for attacks: "If used properly, ISMS enable the organization to keep ahead of the game, responding to the evolving risk environment that the Internet and cyberspace present."

From threats to opportunities

At the business level, it remains a formidable task to model and mitigate threats from all conceivable angles. There's a clear need to use a unified, integrated security system across the whole business and, given the complexity of interrelationships, I asked Prof. Humphreys whether ISMS could apply to small and medium-sized enterprises (SME). "ISMS are applicable to all types of organization and all types of business activities, including those of SMEs. Many SMEs are part of supply chains, so it's essential that they are in control of, and manage, their information security and cyber-risks in order to protect themselves and others." Prof. Humphreys explains that a business's obligations are typically defined in service-level agreements (SLA), contracts between partners of the supply chain that detail service obligations and requirements and establish legal liabilities, and that ISMS often form an integral part of such agreements.



Our private lives may be less complex than global business, but just as much is at stake.

Of course, there are challenges attached to online business for SMEs, but they are far outweighed by the enormous potential that has been opened up by the Internet. It could be argued that it is smaller businesses that have been the most enabled by technology, a point made recently by Ambassador Alan Wolff from the World Trade Organization. Speaking at the 2018 ISO General Assembly, Wolff observed that "anybody – who has a design; who has a computer; who can get on the Web; has access to a platform – can become a part of international trade."

The upsides for social and economic development are enormous: the Internet brings global reach to growing numbers of previously isolated individuals and communities. However, a proven and prudent approach such as ISMS is needed to mitigate the downsides. As Prof. Humphreys reminds me, "a cyber-attack on one part of the supply chain could disrupt the whole of the chain" and the impacts can reach way beyond your own business, or even your direct clients. That's as true for artisan toymakers from Bali as it is for government national health services in Europe.

The right to privacy and the need for confidence

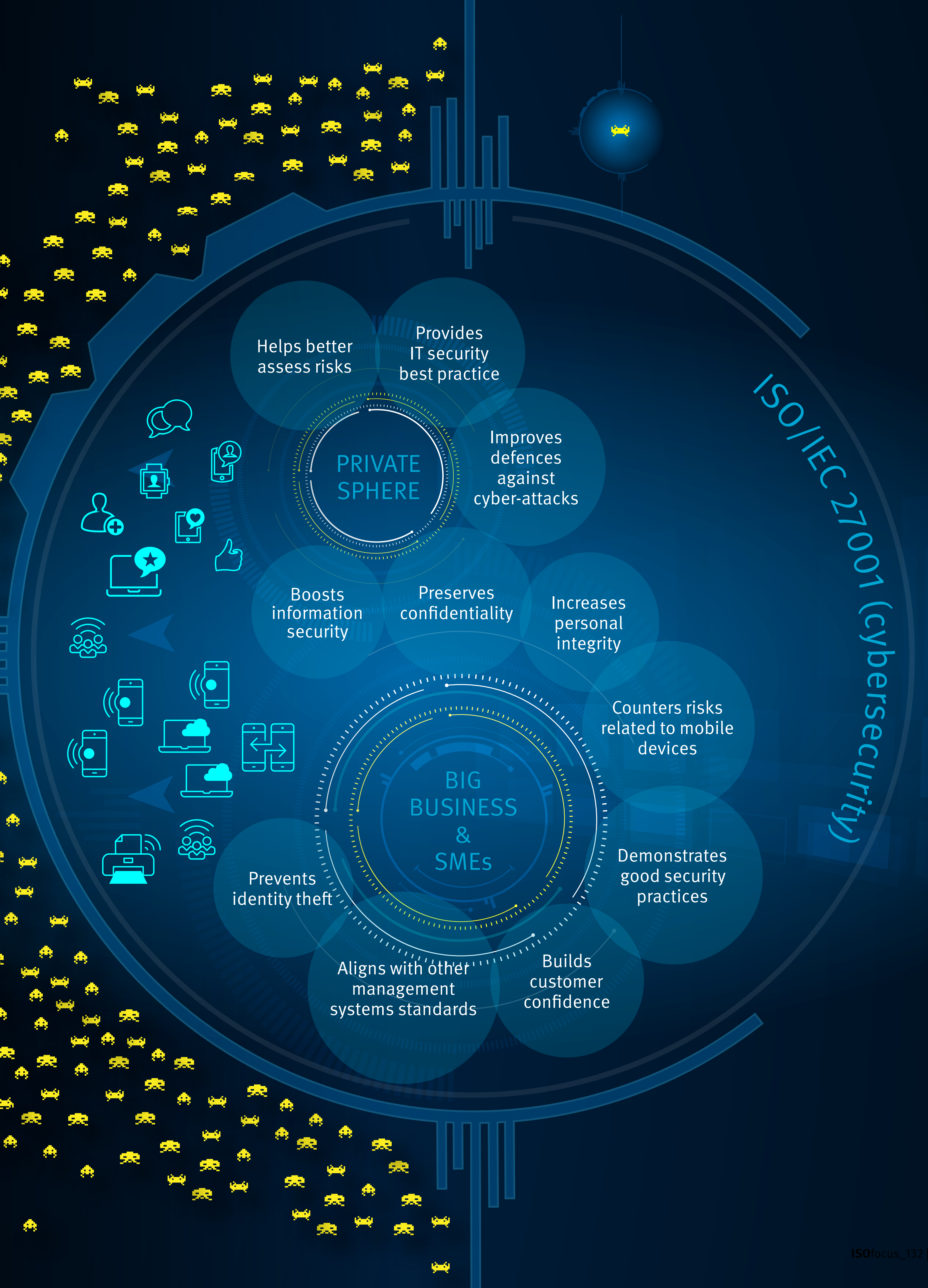
Our private lives may be less complex than global business, but just as much is at stake. For many of us, simply following best practices for passwords and security updates (and bearing in mind that if it smells fishy, or looks too good to be true, then it almost certainly is) should help keep us safe from cybercriminals, much of the time. But people are increasingly asking questions about the way that institutions and companies store, analyse and monetize the vast amounts of data that we hand over more or less voluntarily.

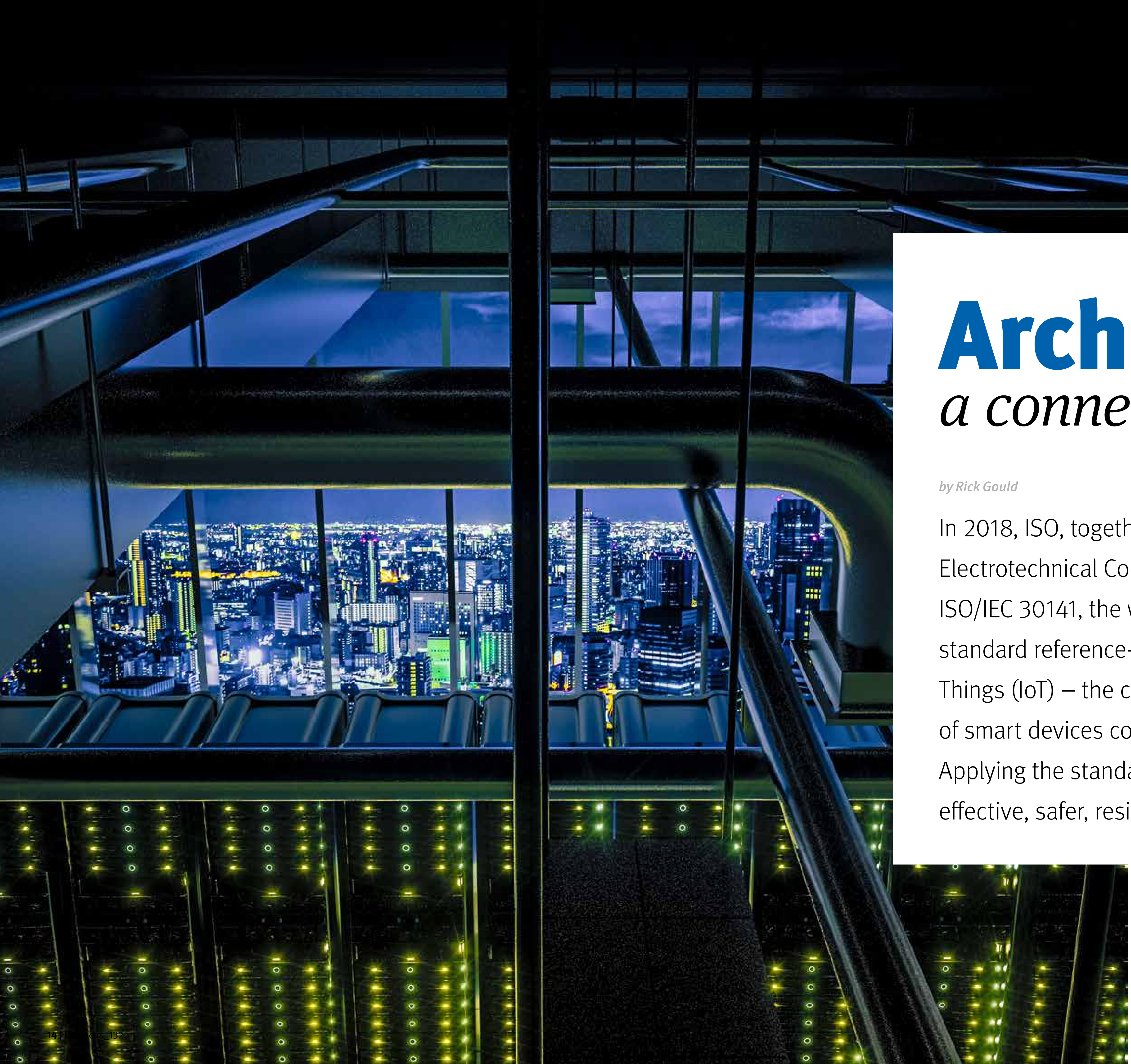
I asked Prof. Humphreys if the ISO/IEC 27000 family provide answers to these sorts of unknowns? "Recently, subcommittee SC 27 has embarked on a new development – ISO/IEC 27552 – which further extends ISO/IEC 27001 to address specific needs of privacy." Currently at the draft stage, the document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving privacy management within the context of the organization.

When privacy, finances, individual or corporate reputation are threatened, it undermines confidence and impacts our behaviour, both online and in real life. The role of the ISO/IEC 27000 family in allowing us to continue to advance is paramount. With many reasons to feel anxious as almost every aspect of our lives becomes digitized, it's reassuring to know that there's a family of standards to count on for information security management systems, and a global group of experts like Prof. Humphreys working to keep us one step ahead. ■

Crack down on cyber crime

The frequency and sophistication of cyber threats are on the rise, wreaking havoc on individuals and organizations alike. ISO/IEC 27001 is fighting back.


ISO/IEC 27001 (cybersecurity)
PRIVATE SPHERE
Helps better assess risks
Provides IT security best practice
Improves defences against cyber-attacks
Boosts information security
Preserves confidentiality
Increases personal integrity
BIG BUSINESS & SMEs
Counters risks related to mobile devices
Demonstrates good security practices
Builds customer confidence
Aligns with other management systems standards
Prevents identity theft



Architecting
a connected future

by Rick Gould

In 2018, ISO, together with the International Electrotechnical Commission (IEC), published ISO/IEC 30141, the world's first harmonizing, standard reference-architecture for the Internet of Things (IoT) – the complex assemblage of billions of smart devices connected through the Internet. Applying the standard will make the IoT more effective, safer, resilient and much more secure.

The IoT is a network of computerized and often wireless devices that allows to see, sense and even control much of the world around us.

It has been an eventful two years since *ISOfocus* first reported on the Internet of Things (IoT) in 2016. Firstly, a new subcommittee was established that focused entirely on developing standards such as ISO/IEC 30141 for this rapidly expanding sector. Secondly, several high-profile attacks on the IoT vividly demonstrated why these standards are essential.

It was about 20 years ago that the British technology pioneer Kevin Ashton coined the phrase the “Internet of Things” when he was working for Procter & Gamble. Ashton demonstrated in a presentation how the company could use radio-frequency identification or RFID – the wireless technique now widely applied in contactless payments and smart ID cards – to track and trace products. And the phrase stuck.

The official definition of the IoT formulated by ISO and the International Electrotechnical Commission (IEC) is “an infrastructure of interconnected entities, people, systems and information resources together with services which process and react to information from the physical world and from the virtual world”. But in simple terms, the IoT is a network of computerized and often wireless devices that allows us, as well as machines, to see, sense and even control much of the world around us, whether at the individual level or to wider, global scales.

Indeed, IoT devices and systems have increasingly found roles in most, if not all, aspects of modern life. Some are already well-known and in common parlance in domestic and consumer markets, yet the largest users of the IoT work within industrial, healthcare, municipal and agricultural sectors. Put simply, any technology prefixed with *smart* is likely to be part of the rapidly growing IoT family; for example, *smart* meters, *smart* cars, *smart* cards, *smart* fitness-trackers, *smart* cities, *smart* phones, *smart* watches, *smart* utilities, *smart* agriculture, *smart* healthcare and even *smart* manufacturing, said to be the next industrial revolution.

Free
19:39
Back
Apple Watch Is Syncing
Your Apple Watch is almost ready.
You'll get an alert when it's finished syncing, so you can use your iPhone as you normally would.
Done
19:39
Press to re
watch face

Bringing us closer

Collectively, the IoT can make us more connected, knowledgeable, efficient, effective and less wasteful. But if handled incorrectly, it can make our computer networks and our data less secure and lacking resilience. For it is the relative simplicity of IoT devices that creates as many challenges as it does opportunities. “The benefits are numerous but, at the same time, the biggest risks are resilience and security,” remarks Francois Coallier, the Chair of joint technical committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 41, *Internet of Things and related technologies*. ISO and IEC founded JTC 1/SC 41 to focus on standards for the IoT, whilst JTC 1 itself is responsible for international standardization in the field of IT and has published well over three thousand standards since its inception in 1987.

The challenges of interoperability – or the ability of IoT devices to connect to each other and other systems in a seamless way – and security are linked. “Technologies are developing all the time and at an extremely rapid pace,” adds Coallier, “so their addition to network has been both fast and often ad hoc as new technologies emerge.” The growth of the IoT is exponential, with the estimated potential of up to 50 billion connected IoT devices projected by 2020 and a market conceivably worth trillions of US dollars.

A CLOUD OF BENEFITS...

> *"There are already many published standards for resilience, safety and security, but ISO/IEC 30141 provides the reference architecture to apply them."*

François Coallier, Chair of ISO/IEC JTC 1, *Information technology*, subcommittee SC 41, *Internet of Things and related technologies*.

A lightbulb year

2016, the same year that saw the founding of JTC 1/SC 41, was also a lightbulb year for the Internet of Things in both the literal and figurative senses, due to some high-profile attacks on networks through the IoT. In March that year, for example, the "Mirai Botnet" attack paralysed much of the Internet on the eastern side of the USA, in the biggest strike on the Internet to date. Many people were surprised at just how fast the malicious code spread and how easy it was for the hacker to get into supposedly secure networks. So how did it happen? It was a case of the weakest link in a chain or, in this case, IoT devices at the edge of a network.

"The Mirai Botnet's creator targeted devices such as wireless CCTV cameras and smart televisions, sold with a limited number of default administrator names and passwords," explains Coallier. The manufacturer made millions of these devices. "The attacking botnet tried each combination of administrator name and password in turn until the attack succeeded, thus permitting the botnet to take control of the device," he says. "With more than a hundred thousand of these devices under its control, the attacker could generate intense denial of service attacks that were able to bring down temporarily part of the Internet in the US."

In another well-documented hack, a factory was sabotaged through a social engineering attack on administrative personal computers (PCs). "In this case, it seems that it was possible from these PCs to access the industrial production systems," adds Coallier, "this would not have happened if the industrial production systems were isolated from the administrative PCs exposed to the Internet through proper network segmentation." More importantly, the network could have been much securer simply by applying well-documented processes and procedures already described in many standards, such as the ISO/IEC 27033 series for IT security techniques, which is one standard prescribing segmented networks for added security.

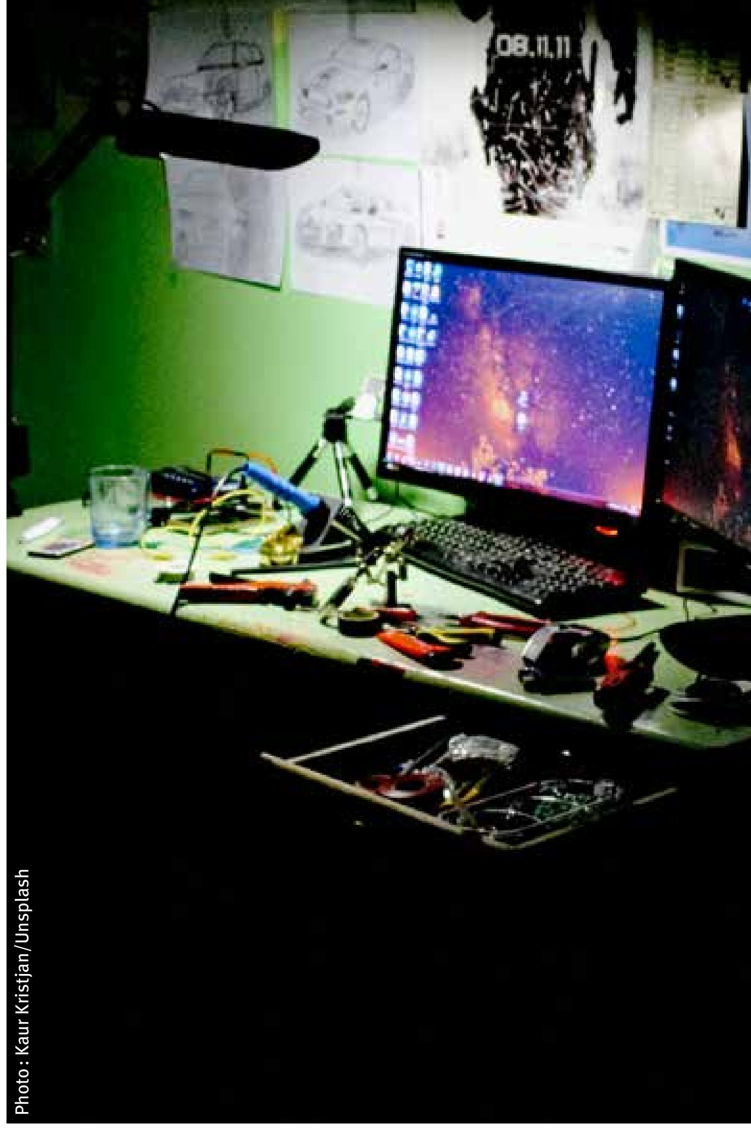


Photo: Kaur Kristjan/Unsplash

> Many people were surprised at just how fast the malicious code spread and how easy it was for the hacker to get into supposedly secure networks.

In the same year as the Mirai Botnet, a group of Israeli researchers demonstrated the potential for hacking into the lighting networks using a modified airborne drone and exploiting a vulnerability in a popular smart lightbulb. Simply through bypassing the security measures in just one lamp, they could infect adjacent, compatible bulbs and then control them. The researchers reported that if there are enough smart lightbulbs present in a city using the same communication protocols, then a malicious attack could easily access and infect the entire network of bulbs within minutes. Whilst this would be an extreme scenario, as a demonstration exercise, it showed the potential for massive malicious attacks in ostensibly secure networks by exploiting overlooked vulnerabilities in simple devices at the edge of a network.

Enter IoT standards

Therein lies the challenge with IoT devices, which is their simplicity coupled with inadvertent ad hoc implementation, compounded if users overlook their security. Many such devices are simplified, low-power mini-computers with a compact operating system based on the widely available Linux, a system popular with computer hackers. This means IoT devices have different requirements from other computers, so when users do not rigorously apply standards for security, these factors make the IoT a growing target for attacks. “It’s a question of yin and yang with the IoT. It provides opportunities, but we need to balance those with careful implementation and pay much more attention to security,” observes Coallier.

Standards for the Internet of Things establish common ground.

This is where International Standards will underpin the operability and resilience of the IoT. How can they do this? The ISO/IEC 29192 series of standards, for example, defines techniques in lightweight cryptography ideal for low-powered, simpler devices. In the lightbulb example, the Israeli researchers recommended a specific security technique described in ISO/IEC 29192-5, which specifies three hash-functions suitable for applications requiring lightweight cryptographic implementations. But as in any developing field, we will need new standards too, and this is the role of JTC 1/SC 41 whose well-rounded scope covers interoperability, safety and, above all, security.

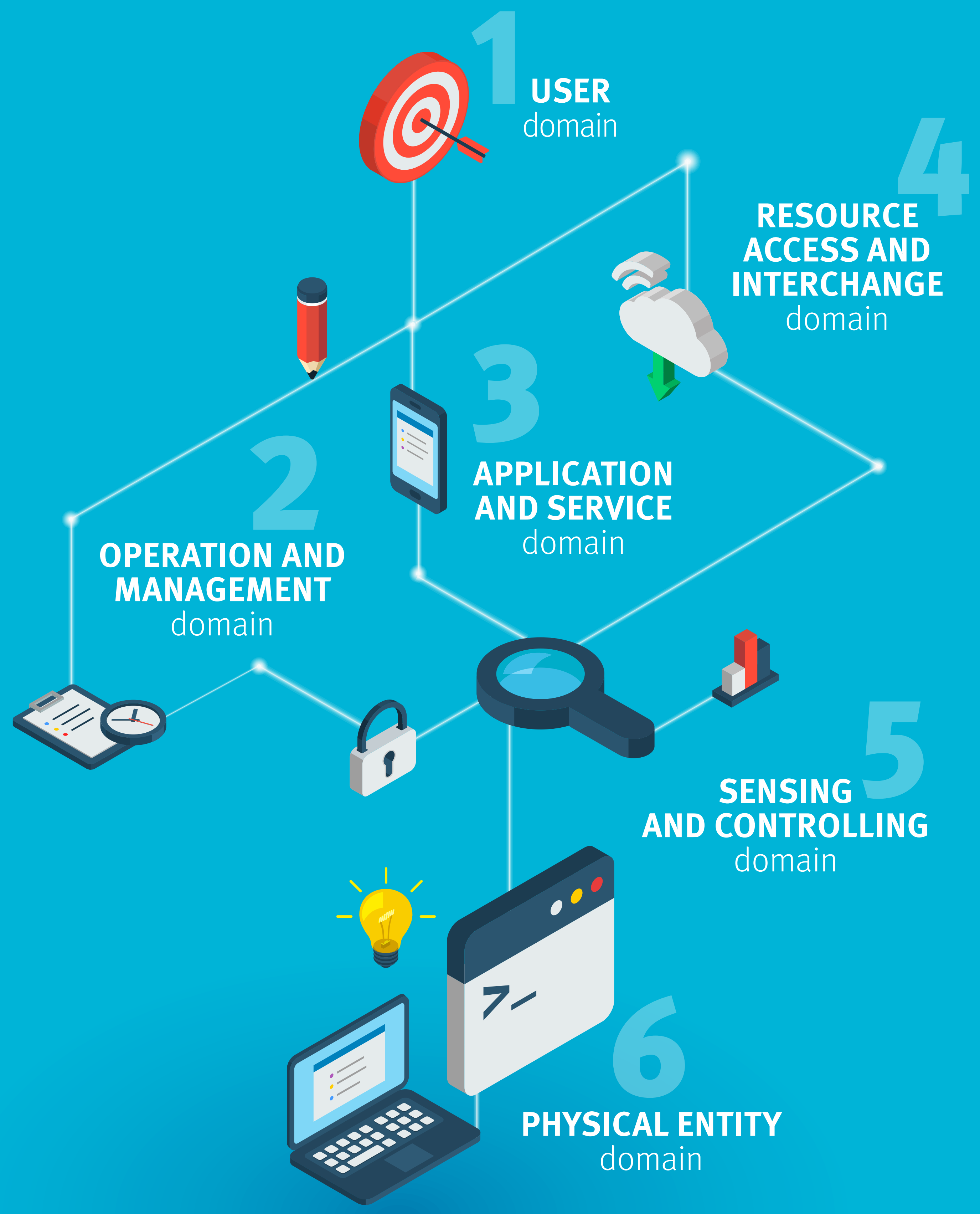
The JTC 1 subcommittee has published 18 deliverables to date, mostly focusing on sensor networks. Included is a guidance note in the form of technical report ISO/IEC TR 22417, *Information technology – Internet of Things (IoT) use cases*, which provides a context for users of IoT standards. This guide covers important issues such as basic requirements, interoperability and standards that users have applied. Most importantly, the examples given clarify where existing standards have a role and highlight where further standardization work is needed.

Building the basics

Standards for the Internet of Things establish common ground regarding topics such as terminology or reference architectures that will help product developers deploy an interoperable ecosystem. ISO/IEC 30141 provides a foundation and reference framework for the many applicable standards produced by JTC 1/SC 41. “We saw a need for a reference architecture to maximize the benefits and reduce the risks,” explains Coallier who is the Chair of the ISO subcommittee. Another foundational standard is ISO/IEC 20924, *Information technology – Internet of Things (IoT) – Definition and vocabulary*. “It is important that those working with the IoT talk the same language,” adds Coallier. ISO/IEC 20924 and ISO/IEC 30141 provide the necessary language.

The working group that developed ISO/IEC 30141 was led by Dr Jie Shen from China, supported by two co-editors who were Wei Wei from Germany and Östen Frånberg from Sweden. Collectively, the project leaders have many decades of experience in the field, enhanced by over 50 other specialists who directly contributed to the standard. “There are a lot of risks and opportunities with the IoT,” informs Dr Jie Shen, adding that “we need to design the perfect maintenance mechanism to overcome these risks; this itself is a matter of detail.”

SIX-DOMAIN MODEL OF ARCHITECTURE FOR THE IoT
ISO/IEC 30141



1 USER domain

2 OPERATION AND MANAGEMENT domain

3 APPLICATION AND SERVICE domain

4 RESOURCE ACCESS AND INTERCHANGE domain

5 SENSING AND CONTROLLING domain

6 PHYSICAL ENTITY domain

Much of the detail is already provided in the many standards published by the JTC 1 subcommittees, and ISO/IEC 30141 supplies a reference architecture to meld them all together, along with several new standards that JTC 1/SC 41 is developing. " ISO/IEC 30141 provides a common framework for designers and developers of the IoT, " explains Coallier. " The standard describes the main characteristics of the IoT, together with a conceptual model and a reference architecture, " he adds. Numerous examples accompany the descriptions.

A six-domain chain

ISO/IEC 30141 also includes a novel and innovative structure known as the Six-Domain Model for IoT reference architecture. This provides a framework for system designers to integrate the multiplicity of devices and operations within the IoT. The project team found that conventional approaches are not suitable for simpler networks. Dr Jie Shen explains : " It is more complicated to build the ecosystem in the IoT, to connect many heterogeneous entities such as human users, physical objects, devices, service platforms, applications, databases, third-party tools and other resources. We found that the conventional layered reference model traditionally applied in IT systems was insufficient." The Six-Domain Model, on the other hand, can help to subdivide the IoT ecosystem very clearly and guide users to establish the new business model of the IoT. The model itself will be even more effective when underpinned by blockchain, the highly secure technique now increasingly used in financial transactions.

The standard also describes a great deal about interoperability – or enabling diverse types of device to communicate seamlessly – and the IoT concept of trustworthiness. This in turn is defined as the degree of confidence users can have that a system performs as expected, whilst ensuring safety, security, privacy, reliability and resilience when faced with disruptions such as natural disasters, faults, human errors and attacks. " There are already many published standards for resilience, safety and security, whilst ISO/IEC 30141 provides the reference architecture to apply them, " informs Coallier. At the same time, as the Internet of Things continues to evolve and grow, JTC 1/SC 41 is developing nine further standards for the IoT, to provide for increasing trustworthiness, interoperability, security and technical specifications. ■

Photo : Ludovic Toinel/Unsplash

THE QUEST FOR cyber-trust

by Robert Bartram

With technology becoming ever more sophisticated and offering both enhanced opportunities and new vulnerabilities and threats, there is a danger that organizations of every different type leave themselves open to malicious attack or data breaches on a massive scale. Risk management, therefore, is just as vital in cyberspace as it is in the physical world. But what are these cyber-risks? How can International Standards help mitigate them? And is it really the case that the only answer is even more sophisticated technology?

The Oxford English Dictionary definition is certainly clear enough: "risk", it says, is "a situation involving exposure to danger". Risk must be taken to achieve results, but also risk must be managed to achieve positive outcomes and avoid negative consequences.

Avoiding risk is impossible. Risks need to be taken and this is an inevitable and necessary part of all our lives, both personally and professionally. Indeed, if any company or organization in any industry in today's highly competitive world was to try and pretend that there were no risks in what they did – in effect, that risk did not exist – then quite apart from defaulting on their statutory and legal obligations, they would very quickly fold and disappear from sight.

But risk can also be a force for good. Managing risks successfully can have positive results, and companies need to take risks in order to achieve their objectives. Organizations quite naturally need a degree of certainty before taking important strategic decisions, and it is essential to understand that risk is really about the likely impact of uncertainty on those decisions. In short, risk is about managing decisions in a complex, volatile and ambiguous world, one that is fast becoming even more complex and ambiguous.

The digital threat

This is particularly true in the field of cyber-risk. In cyberspace, high levels of uncertainty routinely come from addressing issues of national and corporate security. The threat comes not from the context and circumstances of the marketplace, but from "malicious actors" who are attempting serious acts of criminality. They are also, in effect, invisible and like the ghosts and phantoms of ancient folklore, their invisibility merely exacerbates the sense of threat. These malicious actors have both the intent and capability to do harm and are agile and adaptive.

Moreover, technology is becoming more and more sophisticated by the day, if not by the hour. In the past, a successful industrial criminal could perhaps steal a briefcase's worth of documents if they were left carelessly on a desk. Now with USB sticks or exfiltration exploits, the same criminal can steal gigabytes of information that could be the hard-copy equivalent of suitcases all the way to the moon. But it's not just that data storage has become hyper-exponentially sophisticated – from paper to digital – but that the nature and purpose of data has itself changed. If a criminal is intent on stealing protected medical products, for instance, they no longer need to break into a storeroom but can copy the data in digital format and clone the product via a 3D printer.

It is a *sine qua non* that organizations of every shade need "cyber protection" of one form or another. Not only that, they also need a system that is robust enough to alert them to any attack – real or perceived – as quickly as possible. Threats in cyberspace fall into two broad categories: internal and external. To design and successfully execute a protective system from external threats, the emphasis needs to be placed on the intentions and capabilities of external malicious actors – what they are after, why they're after it, and what technologies are available to them.

But organizations also need to prepare for the threat both of malicious insiders and insiders who have mistakenly left the system vulnerable to possible harm. Careless use of personal data can expose an individual to blackmail and recruitment by an organization with nefarious purposes. Organizations can have the best firewalls in the world, but these mean nothing when faced with an insider with high levels of access who can steal information without being detected.

Technology is becoming more and more sophisticated by the day, if not by the hour.

What really counts

So how do governments, businesses and individuals protect themselves from these threats? ISO technical committee ISO/TC 262, *Risk management*, has produced the ISO 31000 risk management standard which creates a framework of principles and process for managing risk in general. Jason Brown is the Chair of ISO/TC 262 and has been, amongst other things, responsible for managing cybersecurity assessment and assurance in the Australian Defence Department. He points out that, as with all risk management, if an organization is serious about protecting itself from cyber-risks, it needs to "go back to the objectives of the enterprise and look at what really counts – in other words, know its digital crown jewels".

Businesses and governments have to carefully assess the value and nature of what they hold dear. For instance, if an organization is the guardian of high-level technical intellectual property in data form, it is obvious that the leaking or theft of such data would have enormous consequences for them. The consequences could, however, be even more destructive if this information were held on behalf of others who are reliant on that organization as part of a supply chain, as a breach in the system could mean the undoing of the entire chain. What counts in the first instance, therefore, is a strategic systemic overview, and not an assessment of the technology itself.

Google returns over **6.5 million** hits in 0.54 seconds when " ISO 31000 " is typed into its search engine.

This approach chimes with that of Dr Donald R. Deutsch, Vice President and Chief Standards Officer of Oracle, based in California, and Chair of technical committee ISO/IEC JTC 1, *Information technology*, subcommittee SC 38, *Cloud computing and distributed platforms*, a group of experts working under the joint stewardship of ISO and the International Electrotechnical Commission (IEC). The cloud, and its position in the hierarchy of risk, has perhaps the greatest immediate significance for everyday consumers. If we use a computer nowadays, it's highly likely we will also be using the cloud. But " cloud computing ", says Dr Deutsch, " is more of a deployment and business strategy than it is a technological strategy ". There are certainly recent technological enhancements that come with risks attached – such as the automatic provisioning of computing resources that are shared by multiple users – yet " the risks are much the same as you would have in any computing environment, but exacerbated and magnified by the scale ".

The price of resilience

International Standards underpin this strategic approach to cyber-risk. As Jason Brown points out, when addressing cyber-risks, the ISO 31000 series should also be assessed in conjunction with the ISO/IEC 27000 series on information security management systems, or ISMS for short. Such an approach balances a focus on technology with that on " human factors ". ISO/IEC 27000 will help an organization assess its purely technological needs, whereas ISO 31000 will help it to understand the value of the information or products it holds in cyberspace, and therefore the degree of technological protection it will need to prevent any attacks. Or to put it another way : a thorough risk assessment using ISO 31000 could save any organization a substantial financial outlay when it comes to purchasing technological security. Ignorance of risk can just as likely lead to paying too much for a protective system as it can to paying too little.

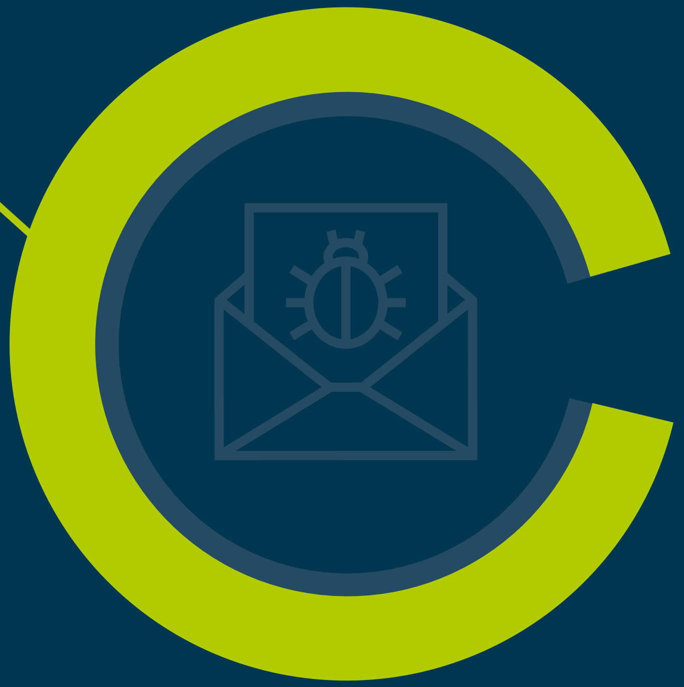
But these two series of standards are by no means the only ones that can help mitigate cyber-risks. Cybersecurity also has to be looked at in terms of business continuity and the ISO 22301 series for business continuity management does exactly that. This series allows for a " documented management system to protect against [...] disruptive incidents when they arise " and enables an organization to assess how its information and telecommunications system supports its objectives and what the consequences would be should it collapse. An organization's investment in cybersecurity may be driven by the level of dependency that it has in the system ; a small organization may be able to continue with (or even return to) paper-based receipts, whereas a giant such as Amazon literally depends on connectivity.

" Cloud computing " is more of a deployment and business strategy than it is a technological strategy.

Likewise, the work of ISO/IEC JTC 1/SC 38 helps producers – and therefore ultimately consumers – speak a common language for cloud computing. Crucially, the demand for this set of standards was not driven, as is usually the case, by the producers or sellers themselves, but by the customers and buyers. Governments and corporations pointed out that each producer was using its own terminology, making it impossible to compare products and make an informed choice about which one to opt for. This led to the publication of ISO/IEC 17789, *Information technology – Cloud computing – Reference architecture*, which established a reference architecture and a framework of common vocabulary. Subcommittee SC 38 also oversaw the creation of ISO/IEC 19086, a four-part standard on service-level agreements between cloud providers and their customers, of which two parts are still in development.

CYBERSECURITY

FACTS AND FIGURES



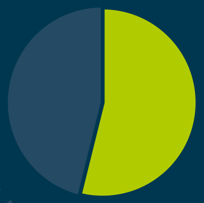
92 %

of malware is still delivered by e-mail

VULNERABILITY OF INDUSTRIAL CONTROL SYSTEMS

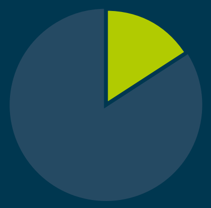
54%

OF COMPANIES SAMPLED EXPERIENCED AN INDUSTRIAL CONTROL SYSTEM SECURITY INCIDENT WITHIN THE PAST 12 MONTHS



16%

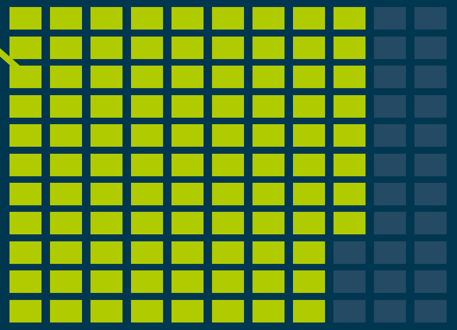
HAD EXPERIENCED THREE INCIDENTS OR MORE



SUCCESSFUL ATTACKS IN 2017

77 %

were fileless



Source : Top cybersecurity facts, figures and statistics for 2018
www.csoonline.com

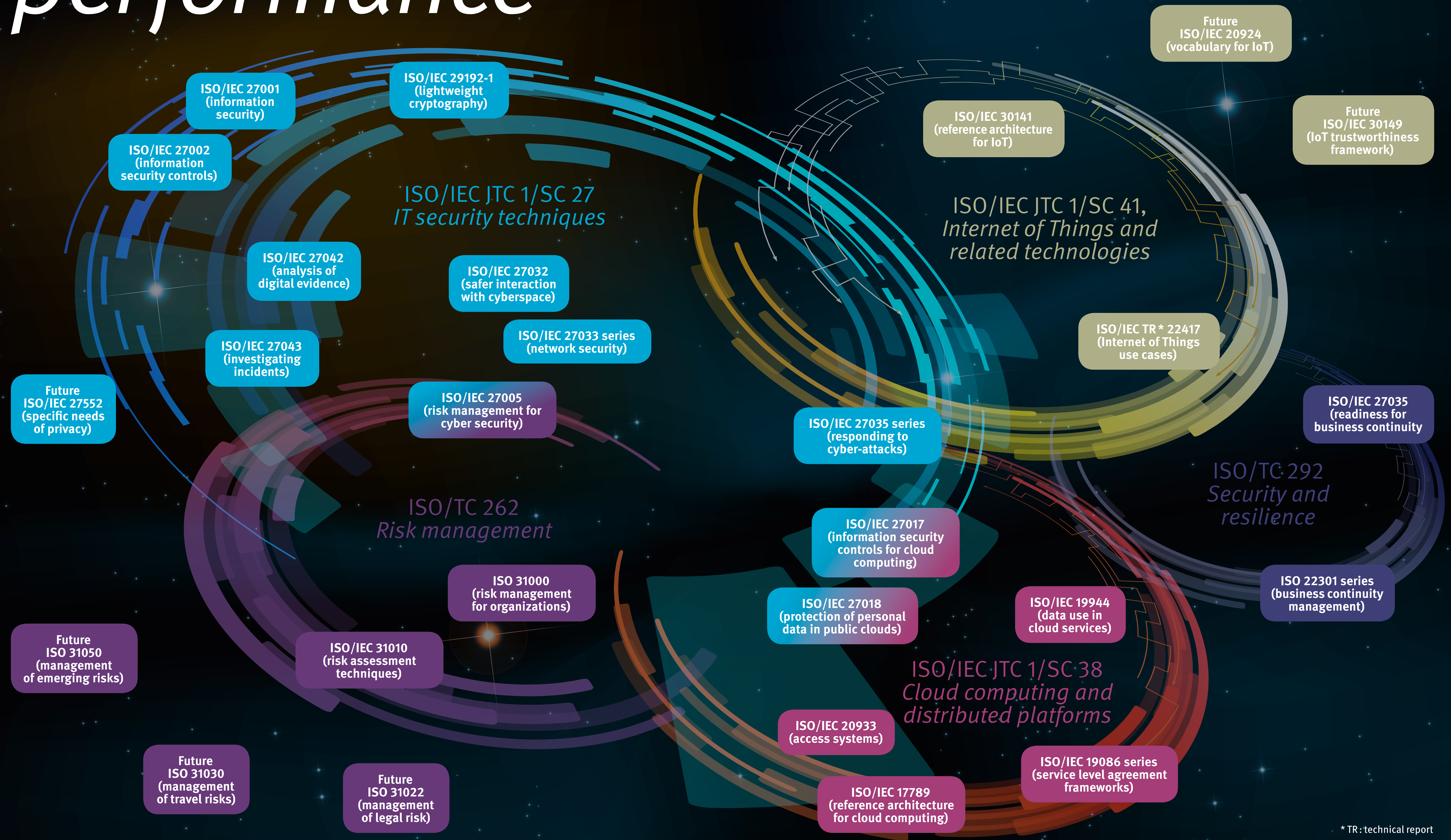
Quantum leap

There can be no doubting the positive impact that all these standards have had on cybersecurity in general and cyber-risks in particular. ISO 31000 has been adopted by approximately 40 countries as their national system for risk management. As if this weren't enough, Google returns over 6.5 million hits in 0.54 seconds when "ISO 31000" is typed into its search engine.

But as technology develops at an ever-faster rate, so International Standards must keep up the pace. The tools that work today may not work in the future. With machine learning moving towards artificial intelligence, for instance, there is likely to be both a learning adaptive capacity and "philosophical" capability in the system which simply do not exist in today's world. Data analytic capability is developing to the extent that large amounts of data can be analysed to pinpoint emerging issues that would not otherwise be detectable. Separately, the advent of quantum computing will also exponentially increase the speed of computing. The conjunction of these three changes in the cyber world will "probably be the most disruptive thing we've had since the discovery of electricity or the atom," says Jason Brown. This doesn't even begin to take into account nanotechnologies or the increasing interconnectivity of all things.

When these factors do eventually combine, the competitive environment for advantage in business, for advantage between countries and not least for advantage between the adversary and the principal, will be massively accelerated. So much so that human input will still probably establish the risk around objectives, but the actual human capacity to deal with cyberspace could be negligible. ISO/TC 262 is currently examining an area it has labelled "Managing Emerging Risks", focusing on those risks that are likely to be the most highly disruptive. As Brown makes clear, both consumers and producers need to approach the future differently, and all of us will "have to be much more open to this highly volatile and highly ambiguous world". ■

Platform for *performance*



ISO/IEC JTC 1/SC 27
IT security techniques

ISO/IEC 27001 (information security)

ISO/IEC 29192-1 (lightweight cryptography)

ISO/IEC 27002 (information security controls)

ISO/IEC 27042 (analysis of digital evidence)

ISO/IEC 27032 (safer interaction with cyberspace)

ISO/IEC 27033 series (network security)

ISO/IEC 27043 (investigating incidents)

Future ISO/IEC 27552 (specific needs of privacy)

ISO/IEC 27005 (risk management for cyber security)

ISO/IEC 27035 series (responding to cyber-attacks)

ISO/IEC JTC 1/SC 41,
Internet of Things and related technologies

Future ISO/IEC 20924 (vocabulary for IoT)

ISO/IEC 30141 (reference architecture for IoT)

Future ISO/IEC 30149 (IoT trustworthiness framework)

ISO/IEC TR * 22417 (Internet of Things use cases)

ISO/TC 292
Security and resilience

ISO/IEC 27035 (readiness for business continuity

ISO 22301 series (business continuity management)

ISO/TC 262
Risk management

ISO 31000 (risk management for organizations)

ISO/IEC 31010 (risk assessment techniques)

Future ISO 31050 (management of emerging risks)

Future ISO 31030 (management of travel risks)

Future ISO 31022 (management of legal risk)

ISO/IEC JTC 1/SC 38
Cloud computing and distributed platforms

ISO/IEC 27017 (information security controls for cloud computing)

ISO/IEC 27018 (protection of personal data in public clouds)

ISO/IEC 19944 (data use in cloud services)

ISO/IEC 20933 (access systems)

ISO/IEC 19086 series (service level agreement frameworks)

ISO/IEC 17789 (reference architecture for cloud computing)

* TR : technical report

Photo : Hal Gatewood/Unsplash

5 things you didn’t know could be hacked

by Elizabeth Gasiorowski-Denis and Vivienne Rojas

More and more common items are becoming connected, making things more convenient not just for us, but also for hackers. Being aware of the dangers in networked devices is the first step to keeping intruders out.

Hackers targeting babies. How on earth could a hacker hack their way into your baby’s room, you ask ? Unfortunately, the sanctity of some babies’ rooms is now being violated... by attackers lurking outside your home. The moral of this story isn’t that your baby monitor could be hacked. The moral is that pretty much every “connected” thing can be hacked.

Photo : es Hicks/Unsplash

Gartner, Inc. forecasts that 20.4 billion connected things will be in use worldwide by 2020. The consumer segment is the largest user of connected things with 5.2 billion units in 2017, which represents 63 % of the overall number of applications used. As we speak, many homes contain dozens of connected things. These include computers, cell phones and tablets, but also many traditional home products such as refrigerators, televisions and security systems.

While conducting a study on the susceptibility of Internet of Things devices to hacking, researchers at Ben-Gurion University in Beersheba, Israel, found many device manufacturers and owners made a hacker's job quite easy. A number of manufacturers set the same default passwords for the same type of device, and often users don't change them. This means that if you have ten network-connected devices and have left one unattended, the whole network is compromised. Frightening indeed.

The truth is, just about anything with a stable Wi-Fi connection can be hacked or exploited by a " professional " hacker. Unless it is a device not attached whatsoever to the Internet, it can be breached in some way or form. This encompasses a very broad range of objects, so let's look at five things that can be hacked !

Baby monitors and cameras

Think of what a baby monitor's purpose is : to monitor young children. This is why this device poses such a threat when hacked and/or exploited. Babies, and even young children, can be watched from disturbing distances by anyone who seizes these devices.

The truth is, just about anything with a stable Wi-Fi connection can be hacked or exploited by a " professional " hacker.

Similarly, many security cameras now connect to the Internet to allow people to access them from outside the home. New York's Department of Consumer Affairs issued a public warning about baby monitor security following a number of widely reported incidents of strangers' voices being heard over them.

Printers and faxes

Printers often have their own Internet connection to allow them to talk to other devices in your home or office, often wirelessly. This connection provides the first step for hackers to remotely access your network. All they need to do is get around any security controls so they can hack their way into your printer and other devices connected to it. Printer vulnerabilities have been well documented, with one hacker claiming to have broken into 150 000 printers in order to raise awareness of their insecurity.

Hackers may also infiltrate your network by sending a simple fax. Since most fax machines today are integrated into all-in-one printers, connected to a Wi-Fi network and a phone line, they can easily be hacked by sending a carefully crafted image file containing malicious code. When converted to data for transmission within the internal computer network, the hidden code can take control of your fax machine, stealing passwords and bank details and hijacking yet more devices.

Photo: Hal Gatewood/Unsplash

Children's toys

Yes, that cute connected teddy bear is a playfield for hackers. It seems that as soon as any device is connected to the Internet, it gets hacked. This includes many objects and appliances that we don't traditionally associate with this kind of technology… such as children's toys. Any Internet-connected toys with microphones, cameras or location tracking may put a child's privacy or safety at risk. That could be a talking doll or a tablet designed for kids. Retailers have been forced to withdraw a number of " connected " or " intelligent " toys after discovering security failures in their Bluetooth and Wi-Fi protocols that could allow a stranger to talk to a child or listen in on conversations. With each of these toys, the Bluetooth connection had not been secured, meaning the attacker did not need a password, pin or any other authentication to gain access.

Retailers have been forced to withdraw a number of " connected " or " intelligent " toys after discovering security failures.

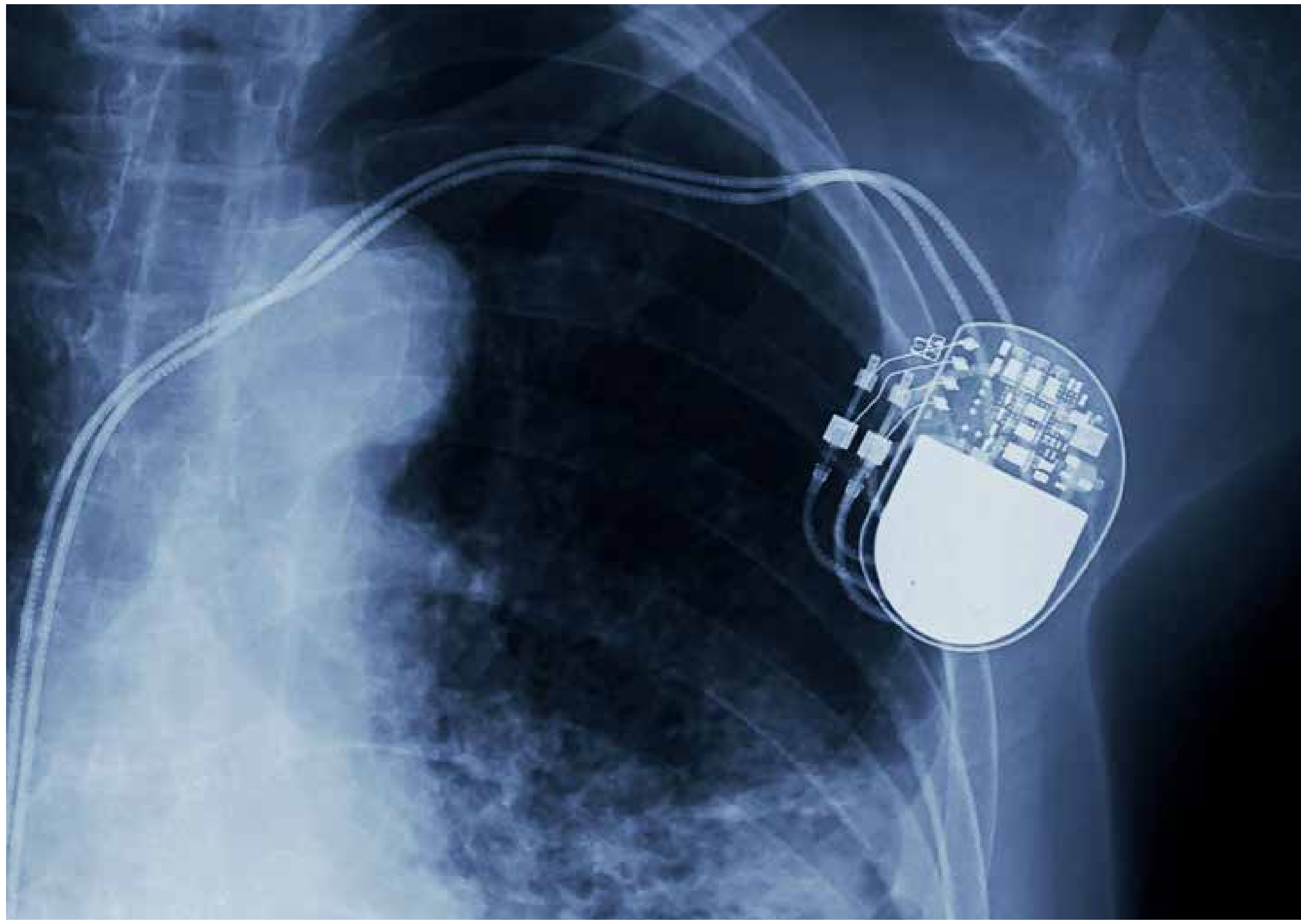
Smart appliances

Your fridge could be your worst enemy when it comes to security. The refrigerator that allows you to send shopping lists straight to your smartphone can be wired in a way that leaves users' Google log-in credentials up for grabs. Any device or appliance in your home that is connected can be a gateway to your entire network. So, while it's convenient to be able to control the temperature of your home while you're out – for example, turning it up when you're ready to leave the office – hackers can control a thermostat and crank up the heat until the owner pays a ransom. Coffee machines are another prime target for cyber intrusion. A flaw in the mobile app that remotely controls your coffee maker could open the door to violations of privacy as hackers steal your Wi-Fi password and sift data transiting through your network.

The US FDA recalled **465 000** pacemakers in 2017 for security problems.

Pacemakers and implants

Hacking your heart is a real thing ! The US Food and Drug Administration (FDA) recalled 465 000 pacemakers in 2017 for fear that security problems might lead to malicious attackers changing the pace of someone's heartbeat – possibly resulting in death. And what about deep-brain stimulation, which feeds tiny precision jolts of electricity into your brain to control your epilepsy or Parkinson's tremors ? This precise control of the brain is an opportunity for hackers to go beyond the more straightforward harms like controlling insulin pumps or cardiac implants. Targeted attacks of brain implants, or " brainjacking ", could cause impairment of motor function, alteration of impulse control, modification of emotions or affect, induction of pain, and modulation of the reward system. So the question remains : Once wireless brain implants become the norm, how do you let the doctors in while keeping the cybercriminals out ?



DID YOU KNOW ?

If you have ten network-connected devices and have left one unattended, your whole network may be at risk!

PRINTERS
TOYS
COMPUTERS
BABY MONITORS
CAMERAS
PHONES
CLOUD
SMART APPLIANCES
PACEMAKERS AND IMPLANTS
COFFEE MAKERS

The consumer segment is the largest user of connected things with **5.2 billion** units in 2017.

Staying safe

There are many other seemingly unlikely ways a hacker can get access to your system. And while you may have the main entrance to the Internet well protected, someone could slip in through the back door. What does this mean for the future? How alarmed should we be with all these smart products attached to the Internet? The answer is *very*. And we don't have to wait until 2020 to experience security vulnerabilities.

Safeguarding our cyberspace is an urgent business and one that needs immediate and ongoing attention. In a number of cases, the right security measures can discourage expert hackers and beat opportunists and, often, International Standards are your first line of defence. Standards like ISO/IEC 27001 and ISO/IEC 27002 provide a common language to address governance, risk and compliance issues related to information security, while ISO/IEC 27031 and ISO/IEC 27035 help organizations to effectively respond, diffuse and recover from cyber-attacks. There are also many other standards defining encryption and signature mechanisms that can be integrated into products and applications to protect online transactions, credit card usage and stored data.

But standards are only good in as far as they are used. So the next time you purchase a baby monitor or any other networked devices, ask yourselves this: Did the manufacturer consider the possibility of hacking? Did the company implement the appropriate International Standards? If the answer to both questions is no, then maybe you should think twice. ■

SIXTY YEARS OF **FIRE SAFETY**

Photo : NEN

ISO/TC 92 delegates in front of the "Het Meisjeshuis" in Delft, an old girls orphanage renovated and reopened in spring 2005 as a cultural meeting place.

Seizing the opportunity of its annual plenary meeting, ISO's technical committee ISO/TC 92, *Fire safety*, celebrated in 2018 its 60th anniversary – six successful decades of producing internationally accepted standards on fire testing, the measurement of fire parameters, fire safety engineering and other related topics. The meeting, which took place last October in Delft, the Netherlands, was hosted by NEN, ISO's member for the country. The Dutch standards organization was commended for its outstanding organization of the event, which included chocolates and petit fours created especially for the occasion.

The festivities ended with a celebratory dinner attended by the Mayor of Delft in person, Marja van Bijsterveldt. She delivered an inspiring speech in which she made ample reference to ISO standards, underlining the importance of standardization in efforts to enhance fire safety. Patrick van Hees, Chair of ISO/TC 92, was later awarded a certificate of merit by NEN Director Rik van Terwisga to commemorate this important milestone.

Standards work was not forgotten amid the celebrations and ISO/TC 92 and its four subcommittees made substantial progress in their different areas of expertise. During the meetings, ISO/TC 92 discussed its potential expansion into new fields such as large outdoor fires, tunnels and underground constructions, and the safety and health of firefighters – a sure-fire sign that the committee will be around for many years to come.

ISO/TC 92 wishes to thank Efectis, FTT-Fire Testing Technology, Kingspan, Etex Group and DGMR for sponsoring these meetings.

ISO STANDARDS SHOWCASED **AT WORLD INVESTMENT FORUM**

At the recent UNCTAD World Investment Forum in Geneva, Switzerland, ISO joined global innovators, development banks, private-sector stakeholders and leading representatives from industry and government to highlight the importance of ISO standards.

More than 80 participants attended the informative session on the theme "ISO standards: helping to make the 2030 Agenda a reality", which aimed to showcase the role of standards in achieving the Sustainable Development Goals (SDGs), the United Nations agenda to secure world peace and prosperity by 2030. With an interactive programme including a panel and discussion, the event also provided a platform to exchange experiences on such areas as international trade and public policy challenges. Organizations and companies looking to contribute to the SDGs will find that International Standards provide effective tools to help them rise to the challenge.

The ISO session was among some 60 events that included three summits, five ministerial roundtables, private-sector-led discussions and several awards ceremonies. The collective goal of the Forum, organized by UNCTAD every two years, is to strengthen cross-border cooperation in the interest of promoting international investment and its contribution to economic growth and development.

For more information:

http://worldinvestmentforum.unctad.org/iso

LAUNCHING ISO 55002 ON ASSET MANAGEMENT

The new edition of ISO 55002 was officially launched in Amersfoort, the Netherlands, by ISO/TC 251, ISO's technical committee on asset management. The launch became official when committee Chair Rhys Davies and Convener Ton van Wingerden symbolically presented the inaugural copy to Anton van der Sanden, Director of Royal HaskoningDHV NL. The engineering consultancy headquarters was hosting the week-long meeting of ISO/TC 251, tasked with developing the ISO 55000 suite of standards on asset management systems.

A pivotal part of the series, ISO 55002 offers guidance for the application of an asset management system in accordance with ISO 55001. Based on feedback and experience from early adopters of the standard, this important revision contains guidance on creating a strategic asset management plan, processing risk in asset management and applying ISO 55001 to organizations of all sizes. Drawn up by a group of international experts from 30 countries, many of whom were instrumental in drafting ISO 55001, this is a solid document that remains true to the spirit of the original requirements while building on worldwide feedback of using the standard.

First published in 2014, the ISO 55000 suite includes three standards whose relevance and popularity have been illustrated many times over. Of the series' success, Rhys Davies commented that ISO 55000 explains "why" an organization needs an asset management system, ISO 55001 covers "what" it needs to do to conform to the standard, and ISO 55002 offers guidance on "how" to comply with the standard's requirements. He believes the ISO 55002 update will significantly advance the adoption of this management system around the world.

Photo : NEN

ISO/TC 251 Chair ***Rhys Davies*** (right) *and Convener* ***Ton van Wingerden*** (left) *present the first copy of ISO 55002:2018 to* ***Anton van der Sanden****, Director of Royal HaskoningDHV NL.*

EMPOWERING **THE PHILIPPINES**

ISO Secretary-General Sergio Mujica joined the Bureau of Philippine Standards (BPS), ISO's member for the Philippines, in celebrating its annual National Standards Week in Manila. Held to coincide with World Standards Day, which is celebrated each year on 14 October in tribute to the collaborative efforts of experts worldwide who develop International Standards, the week kicked off with a standards essay writing contest and a poster making contest for some 150 high-school students from schools in and around the capital.

In his informative presentation, Mujica gave an overview of ISO history and the ISO standardization system, enumerating the many benefits that standards bring to government, the economy and consumers as well as their constructive impact on technological progress. He noted the Philippines' low participation in ISO standardization programmes due to lack of resources and ended with a powerful message for students to become the standards professionals of tomorrow.

During his two-day visit in Manila, the ISO Secretary-General met with members of the Philippines Congress and some notable standards professionals to discuss a proposed national quality infrastructure, which is highly supported by BPS and would help the country on its way to achieving economic development.

Photo : BPS

ISO Secretary-General ***Sergio Mujica*** *takes a "groufie" (group selfie) with students in Manila.*

TALKING TOILETS
WITH BILL GATES

"International Standards are key to the progression of new sanitation technology and developing an industry that saves lives," said Sergio Mujica at the Reinvented Toilet Expo held last October in Beijing, China. The ISO Secretary-General was speaking on a high-level panel that featured Bill Gates, Co-Chair of the Bill & Melinda Gates Foundation, and Dr Jim Yong Kim, President of the World Bank, as well as other high-profile figures from industry and government.

The three-day summit, supported by the Gates Foundation, discussed the global perspectives of non-sewered sanitation, a new stand-alone toilet technology that safely treats waste without the need to be connected to a traditional sewerage system. The offerings at the Expo ran the gamut from toilets with biological and chemical processes to membranes that filter liquids, designed to enable more people in developing regions to go to the bathroom safely and with dignity.

Bringing about this revolution is no mean feat, but the technology can now be supported by a new International Standard dedicated to non-sewered sanitation systems. By providing safety and performance requirements for integrated treatment units, ISO 30500 not only facilitates their effective manufacture, but contributes to the development of the sector as a whole, ensuring billions get the safe sanitation they need to lead healthy and productive lives.

Photo: Gates Archive

***Bill Gates** shares the stage with a jar of human faeces as he showcases the benefits of new toilet technologies.*

ISO/AOAC COOPERATION EXPANDS

ISO and AOAC INTERNATIONAL (AOAC) announced in 2018 the renewal of their cooperation agreement for the joint development and approval of common standards and methods. First signed in 2012 for a five-year term, the high-level partnership with AOAC, a non-profit scientific association committed to producing reliable chemical analysis methods, is destined to significantly increase the global relevance of the respective organizations through the adoption of common standards approved by Codex Alimentarius.

Under the new agreement, AOAC and ISO can participate in each other's work and engage in joint standards development through working groups comprising AOAC and ISO experts. Subject to parallel approval processes for AOAC and ISO, the resulting standards would then be published by both organizations.

The cooperation, which focused originally on milk and milk products, will extend its purview to encompass projects within the scope of ISO technical committee ISO/TC 34, *Food products*. Future priorities for AOAC/ISO standards may include more work on nutrient analysis, as well as expanding to contaminants, adulterants and pesticide residues, for the good of all stakeholders in the food industry.

ISO FORMS PARTNERSHIP WITH WORLD BANK GROUP
TO HELP COUNTRIES FACILITATE TRADE

ISO has partnered with the World Bank Group (WBG) to support ISO member national standards bodies in developing countries, based on their needs, with the implementation of the World Trade Organization (WTO) Trade Facilitation Agreement (TFA). This will cover areas such as applying good practices for technical barriers to trade and, in particular, implementing conformity assessment procedures.

The partnership arrangement was made at a border agency cooperation workshop that took place from 14 to 16 November 2018 in Cape Town, South Africa, where ISO was invited to present on "Standards and trade facilitation".

The event brought together senior officials from 12 African countries involved in the implementation of the TFA to share experiences and learn from each other. It was organized by the WBG, the WTO Secretariat, the International Plant Protection Convention (IPPC) Secretariat, the World Organization for Animal Health (OIE), the Food and Agriculture Organization (FAO) and the World Customs Organization (WCO).

The WBG's Trade Facilitation Support Program actively supports developing countries to align their trade facilitation laws, procedures and processes to enable implementation of the TFA.

In most developing countries, the ISO member, or national standards body (NSB), is the national enquiry point as required by the WTO Agreement on Technical Barriers to Trade, and may also be a provider of conformity assessment services.

At the event, ISO also committed to provide the WBG with inputs on its TFA-related tools that apply to the activities of NSBs.

ADVANCING THE GLOBAL AGENDA
– CALENDAR 2019

The United Nations Sustainable Development Goals (SDGs) offer a vision of a fairer, more prosperous, peaceful and sustainable world. With its expertise and resources, ISO is well positioned to support its members in achieving the SDGs, all of which are related to ISO's work.

Find out how ISO standards contribute to the 17 SDGs by downloading the ISO 2019 Calendar. Designed in a 17-month format, it showcases some of the many ways in which ISO can make the 2030 Agenda a reality – so no one is left behind.

The ISO 2019 Calendar is now available to download on iso.org.

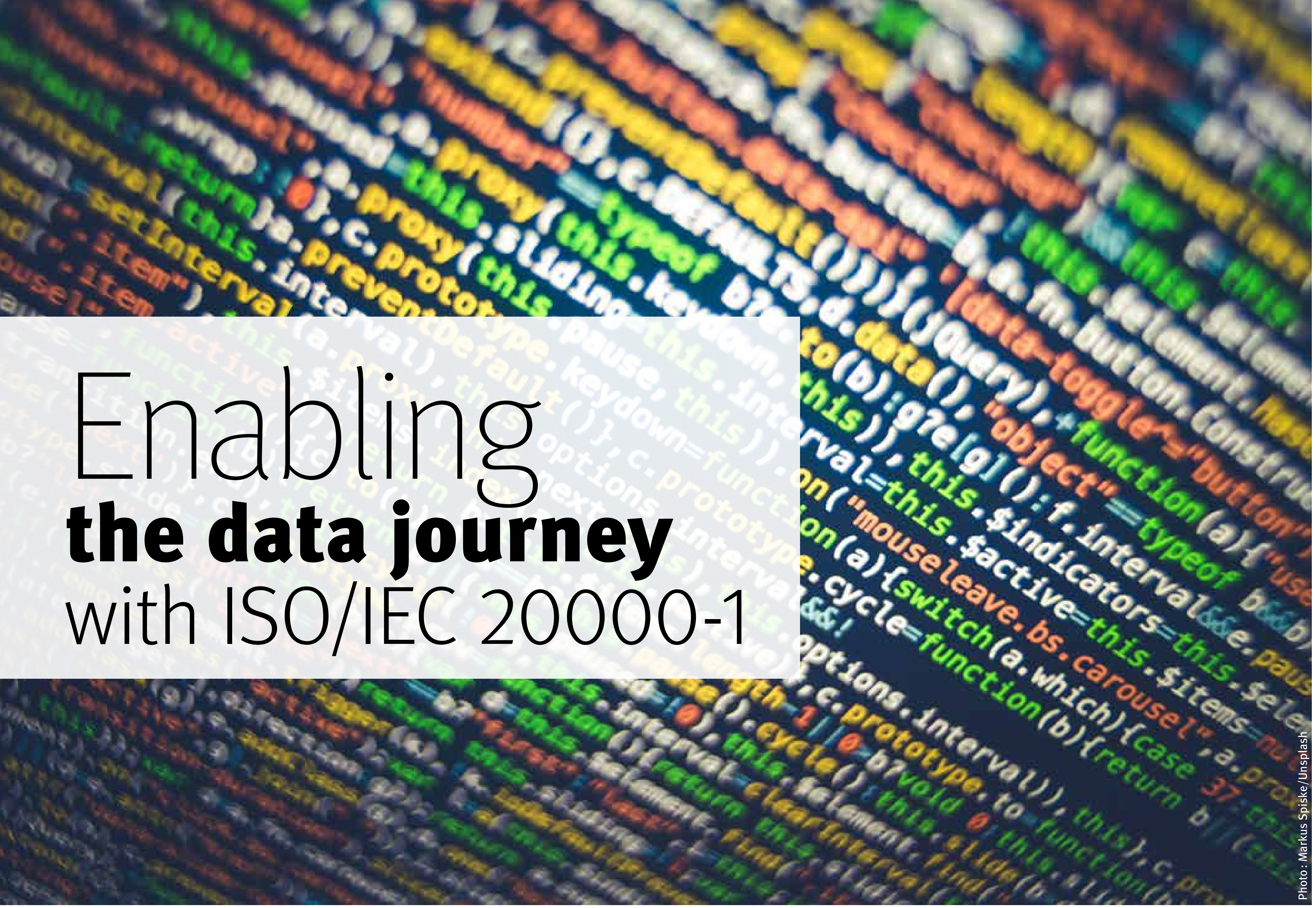


Photo : Markus Spiske/Unsplash

Enabling **the data journey** with ISO/IEC 20000-1

Data, and the cloud that hosts it, has an almost infinite value for businesses that know how to process it – as long as the proper strategy is in place to unleash its potential. Orange Business Services helps customers turn their data into a true business asset, thanks to a little assistance from ISO/IEC's IT service management standard.

With the digital revolution, businesses are producing more data than ever before. This data is no more than a raw material, but an organization's ability to transform it into useful information can unlock a world of opportunities. Thanks to cloud computing, organizations can have access to powerful IT capabilities – and with more flexibility than ever, they can externalize all or part of their information systems, workspaces, servers, applications and storage.

Although the cloud has been around for over a decade, the biggest objection still hindering its adoption is ongoing concern about data security and integrity. Systems integrators that can successfully offer cloud-hosted security and access control solutions will find themselves well-positioned for the future, with the ability to deliver a wide range of managed and remote services to customers while boosting the overall value of their company.

Orange Business Services is one such company. As the B2B branch of the Orange Group, which boasts 260 million customers across 28 countries and an annual sales revenue of EUR 41 billion, the global ICT provider aims to be a leading performer in the "data journey". Supporting organizations through every step of their digital transformation, it offers customers expertise in the collection, transfer, security, storage, processing, analysis and sharing of data, and value creation. To deliver support on such a broad scale, Orange Business Services needs to operate seamless global processes managed under a corporate governance model that applies worldwide.

The implementation of ISO/IEC 20000-1, *Information technology – Service management – Part 1 : Service management system requirements*, was thus a logical objective. Developed by ISO and the International Electrotechnical Commission (IEC), the flagship standard of the ISO/IEC 20000 family helps organizations embed a service life-cycle strategy, providing best practice on how to manage their portfolio of services so they remain current. The release in 2018 of a new and improved edition prompted us to ask Jean-Pierre Girardin, Customer Services & Operations at Orange Business Services, how this latest update will help the company in its commitment to maintain superior end-to-end services – wherever its customers do business.

***ISOfocus* : What are the reasons for the enthusiastic uptake of ISO/IEC 20000-1 by Orange Business Services ?**

Jean-Pierre Girardin : With over three thousand renowned multinational corporations at the international level and over two million professionals, companies and local communities in France, Orange Business Services relies strongly on information security standards and the company has been certified to ISO/IEC 20000-1 for ten years.

A conscious decision was made from the beginning to introduce the standard progressively and in an integrated manner. So we built on our initial corporate quality management systems based on ISO 9001 to enhance our service management processes in an integrated framework. This allowed us to align our service processes across our Orange Business Services operating sites all over the world.

As a B2B services-oriented company, getting certified to ISO/IEC 20000-1 was a golden opportunity. It enabled us to focus on improving our services and benefit from the virtuous combination of three management systems standards – ISO 9001 (quality), ISO/IEC 20000-1 (IT services) and ISO/IEC 27001[1] (information security) – and the continuous improvement loops inherent in all three standards.

[1] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*, was developed jointly by ISO and the International Electrotechnical Commission (IEC).

What are the major benefits that ISO/IEC 20000-1 has brought Orange Business Services ?

The implementation of ISO/IEC 20000-1 has provided a number of key benefits, both internal and external. Our triple certification, which is renewed each year with regular new extensions of scope, identifies Orange Business Services as a trustworthy and reliable partner and recognizes the quality of our management system globally. We have since also added ISO 14001 for environmental management in three of our sites. All our indicators show that customer satisfaction has significantly increased as a result of these efforts. What's more, the certification programme has proved an excellent way of reinforcing team cohesion among our staff, which has enabled us to keep up the momentum over the years.

The increasing uptake of ISO/IEC 20000-1 isn't particularly surprising when you consider today's security concerns. Could you please elaborate on the standard's additional security-related benefits ?

ISO/IEC 27001 for information security covers a defined scope of our activities and entities (operational, cloud services...), so we have ISO/IEC 20000-1, Paragraph 6.6 on information security management, to thank for securing the breadth of our processes and activities on three levels : requirements in our services, security controls in our operations, and a portfolio of managed security services.
For instance, we proactively monitor and respond to security incidents that could conceivably affect assets entrusted to us. To this end, we ensure that all changes are assessed before implementation to prevent any potential impacts on security protection. We have also introduced robust security controls in our processes and working procedures that have proved very effective. The additional security features of ISO/IEC 20000-1 also contribute to raising awareness of security as a full part of operational practice and auditors have acknowledged the exemplary behaviour of our staff when it comes to protecting the integrity of data.

How is ISO/IEC 20000-1 integrated at the process, operational and strategic levels within Orange Business Services ?

ISO/IEC 20000-1 was fully integrated from the very beginning of the project in 2008 into a global coherent security management system. This was especially important as it coincided with the beginning of the ISO/IEC 27001 certification of our Egypt Major Services Center in Cairo, which was later followed by the India Major Services Center in Gurgaon near Delhi and, finally, our operations in France, Brazil and Mauritius. As a result, the ISO/IEC 20000-1 requirements have become part and parcel of all our processes and activities, whether it be in our relationships with customers, our activities with suppliers or throughout the services life cycle, from order to delivery.
At the strategic level, Orange Business Services conducts regular management reviews on a local, regional and global scale, where our certification results are carefully monitored. We anticipate customer expectations and adjust the scope as dictated by the business.

Photo : Orange Business Se

Being so successful in implementing ISO/IEC 20000-1 mainly by internal resources, could you share some tips with *ISOfocus* readers ?

It is important to take a step-by-step approach when seeking certification. We began by forming a skilled, knowledgeable and dedicated team to manage the project. In this regard, proficiency in the ITIL framework, which helps align IT services with business needs, was considered a plus. We felt it was important to run a methodical gap analysis and feasibility study before introducing any new service for certification and reinforced our pool of internal auditors to help validate our progress through annual audits of all our processes and entities.
To create momentum among the staff, we also organized awareness sessions on ISO/IEC 20000-1 and all aspects related to certification and standards. Remaining pragmatic at all times, we aimed to convey the benefits of a certification journey to make sure everyone properly understood the purpose of implementing the standard. The trick is not to talk about the standards' requirements, but rather to concentrate on showing the importance of applying them for the benefit of our customers, our services and our processes. The whole enterprise was of course endorsed by senior management, which was crucial to its success.

A new version of ISO/IEC 20000-1 has been recently published – any thoughts on the way forward ? Future projects/plans ?

The new version of ISO/IEC 20000-1 opens exciting perspectives for Orange Business Services. The standard is aligned to the new High-Level Structure used across all ISO management systems standards, including ISO 9001:2015, ISO/IEC 27001:2013 and ISO 14001:2015, so this version will be even easier to understand.
We are already looking at how to accommodate the changes within Orange Business Services and aim to be one of the first companies to successfully implement the new edition of the standard. This will be our challenge for 2019 ! ■

Photo : Orange Business Services

***Jean-Pierre Girardin**, Customer Services & Operations at Orange Business Services.*

Thanks to cloud computing, organizations can have access to powerful IT capabilities.