ERMA | ENTERPRISE RISK MANAGEMENT ACADEMY

RISKVIEW

RISKVIEW MAGAZINE #4 | DECEMBER 2015

SURVIVING THE DIGITAL WORLD:

RISKS THAT BIND THE FUTURE

RISKVIEW Magazine is a quarterly publication on risk management managed and released by ERMA (Enterprise Risk Management Academy).

riskviewmagazine.com

WHAT THEY SAY

"Information technology and business are becoming inextricably interwoven."

Bill Gates
The founder of Microsoft

"If you go back a few hundred years, what we take for granted today would seem like magic."

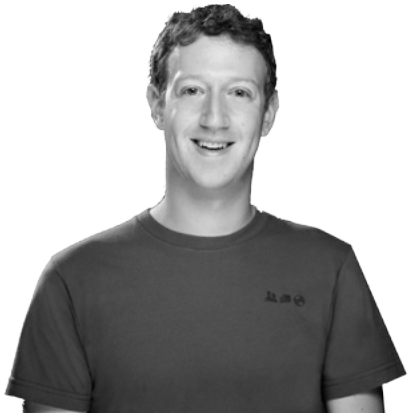
Elon Musk
The founder of Tesla, SpaceX and Paypal

"Technology is nothing. What's important is that you have faith in people."

Steve Jobs
The founder of Apple

"In a world that is changing really quickly, the only strategy guaranteed to fail is not taking risks."

Mark Zuckerberg
The founder of Facebook



WELCOME TO THE FOURTH EDITION OF RISKVIEW MAGAZINE

Colin Adams
ERMA Advisory Board

Welcome to the latest edition of RiskView Magazine. In this edition, we look at a variety of risk topics which we are confronting, including data security and the impact of new technologies such as drones and driverless vehicles. With recent revelations from senior officials in the US that the "internet of things" could be used for surveillance purposes, the combination of new technologies and the security challenges they pose will likely increasingly impinge on our daily lives including into our homes and other private spaces. Both companies and individuals need to respond to the growing challenges posed by digital technologies and security; in companies this might drive the need for new skill sets in the Executive ranks. This edition also includes a futurist's perspective on the future role of humans as technology, and artificial intelligence, continue to develop at exponential rates.

IN THIS EDITION

HAS EASE MADE US LESS SECURE?

By Ashley Wong

The need to remember increasingly complex passwords so you can go about your daily business online is a real problem for many users. Therefore, having a piece of software do the job for you is unerringly appealing. However, when a company that specializes in providing password management services recently announced that it had been hacked, serious alarm bells began to ring.

Having a cloud-based vault in which to store all your passwords so you can automatically enter any password protected site at which you are registered is a brilliant solution for most web users. But, as with all things digital, there is a potential disadvantage to having all your security eggs in one basket. In this case, while the password security company was able to affirm to its customers that all the data stored in its vault were safe, it could not offer the same assurance about the master passwords used to access the vault.

The solution offered by the company was for all of its customers to change their master password, but this was far from reassuring or convenient. Worse, it does not begin to deal with the inherent risk in the system: the security offered by the use of a single master password.

This is clear when you compare the single password method with the security surrounding the protection of a safety deposit box held within a physical bank vault. For maximum security, a key is given to each customer for their box while the bank holds a master key. In order to access the box, both the customer and the bank must use their keys.

In the digital world, the only way to replicate this real-world approach is to use multi-factor authentication: in other words, two passwords. This is achieved by having the customers access their account with both a master password and a code generated by a third-party app. This simple solution could well be the only way for the security company to provide a robust level of data protection to its customers.

HAS TECHNOLOGY STRIPPED US NAKED?

By Meredith Evelyn

No matter who you are or where you work, your personal information is no longer 100 percent safe. Even if you do not use Facebook or Instagram, hackers can get access to your social security number (or equivalent), date of birth, and home address. This is because your employers keep this information online – and they are frequently hacked.

Digital theft is no small matter and the consequences can be serious. It can take up to 6 months to clear up the mess resulting from fraud and identity theft and, years later, security checks can result in false reports identifying you as a criminal or security risk.

However, the primary use for stolen personal data is phishing scams. These are attempts to trick you into logging into your bank account or resetting your password for an account using a link supplied by the hacker. They are usually delivered via email or text message. Phishing is most effective when it is personalized, so a message that appears to come from a trusted person or that includes details of a legitimate bank account means you are more likely to be fooled. This is what makes your personal data so vulnerable.

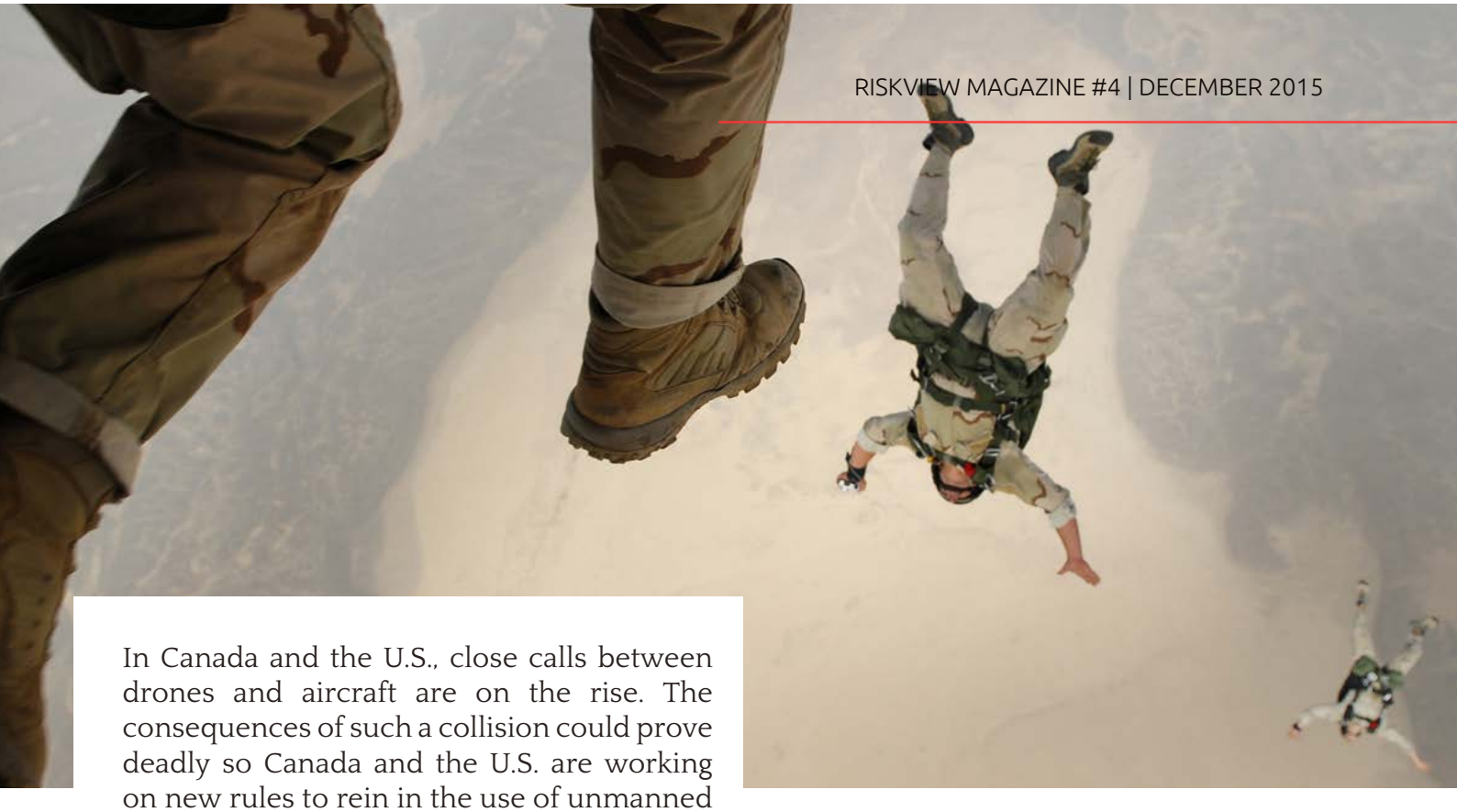
The best way to counter phishing scams is to be alert and cautious. Never open a link to any account sent in an email. Close your browser then re-open it as a new browser window then go directly to the site in question. Any important messages will be on your account. Another way to safeguard yourself is to keep software such as web browsers, Adobe Acrobat, Flash, and Oracle's Java up to date as

older versions often contain security holes that can be exploited by hackers.

Finally, monitor your credit information. Get a free credit report from suppliers such as Equifax, Experian or TransUnion (in the US) so you have a clear picture of your credit health. You can even get alerts sent if anyone attempts to defraud you or steal your identity.

FLYING INTO TROUBLE

By Willis Hudson



In Canada and the U.S., close calls between drones and aircraft are on the rise. The consequences of such a collision could prove deadly so Canada and the U.S. are working on new rules to rein in the use of unmanned aircraft in our increasingly crowded skies.

In Canada, if you want to operate a drone or unmanned aerial vehicle (UAV) heavier than 25 kg for either commercial or research purposes, Canadians need to get a Special Flight Operations Certificate (SFOC) from Transport Canada. Although permission is not required to fly a smaller drone for recreational purposes, hobbyists are expected to follow Transport Canada's safety guidelines. These forbid the flying of drones near airports, buildings, populated areas or moving vehicles.

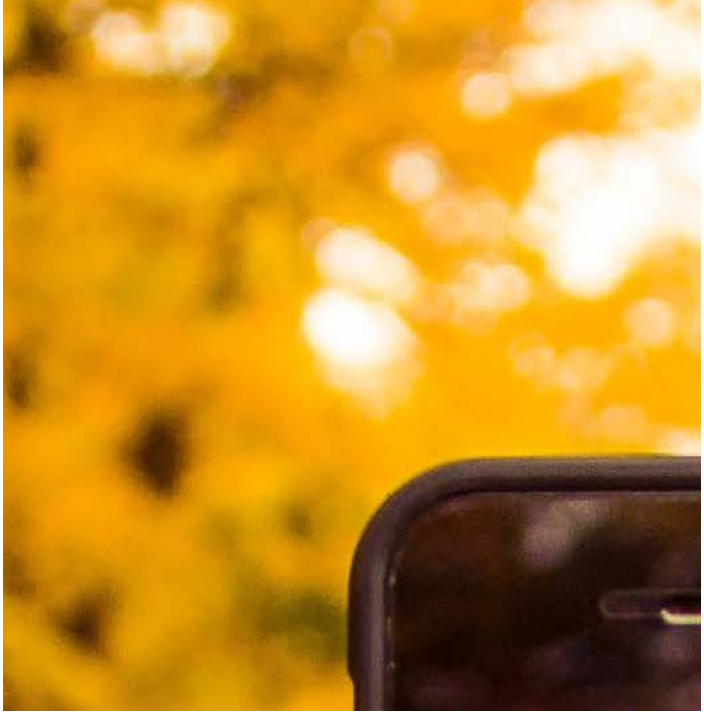
The problem is that not everyone who buys a drone is aware of these rules. As Jeremy Laliberté, professor of mechanical and aerospace engineering at Carleton University in Ottawa points out, the current rules were drafted when very few people had access to drones. He asserts that Transport Canada needs to create better public awareness about its safety guidelines.
Commercial and research drone operators present less of risk than leisure users as they are better educated about the rules, and because they have to obtain SFOCs from Transport Canada. They also have to inform the government as to what kind of drones they are using, where they are using them and why.

When it comes to using SFOCs for research and commercial purposes, Canada is a world leader and issued 1,672 licenses in 2014 alone. By comparison, the U.S. has only recently starting to regulate unmanned aircraft and has only issued 1,000 approvals for commercial and research drones, despite having many more academic and research institutions.

The U.S. Federal Aviation Administration has announced the creation of a task force to develop a registration system for drones while Canada is looking to bring in updated drone regulations, replacing its existing guidelines with stricter rules requiring licensing, training and registration.

HOW HEALTHCARE NEEDS TO RETHINK SECURITY IN THE DIGITAL AGE

By Kendal Randy



According to a recent HIMSS report, there has been a noticeable shift since 2008 from a compliance-based approach to cyber security to one focused on risk management in the healthcare industry.

As stated in the report, the message that mere HIPAA compliance does not offer enough security against hacking seems to have sunk in. As the researchers wrote, "Many healthcare organizations now realize that achieving a secure IT environment is not a 'one and done' endeavour, but rather is an ongoing effort."

The report tracks responses to the annual HIMSS Cybersecurity Survey, which was first released in 2008. At this time, the focus was on understanding how health organizations (who were new to the task of storing large amounts of digital data) were managing to protect their patient information.

At the time, half of the providers said that they conducted risk assessments at least once a year, and most said they were meeting compliance requirements. More recently, the situation has changed due to the incidence of larger and more expensive data security breaches. In fact, in 2015 alone, hackers compromised more than 100 million patient records using advanced and persistent attacks.

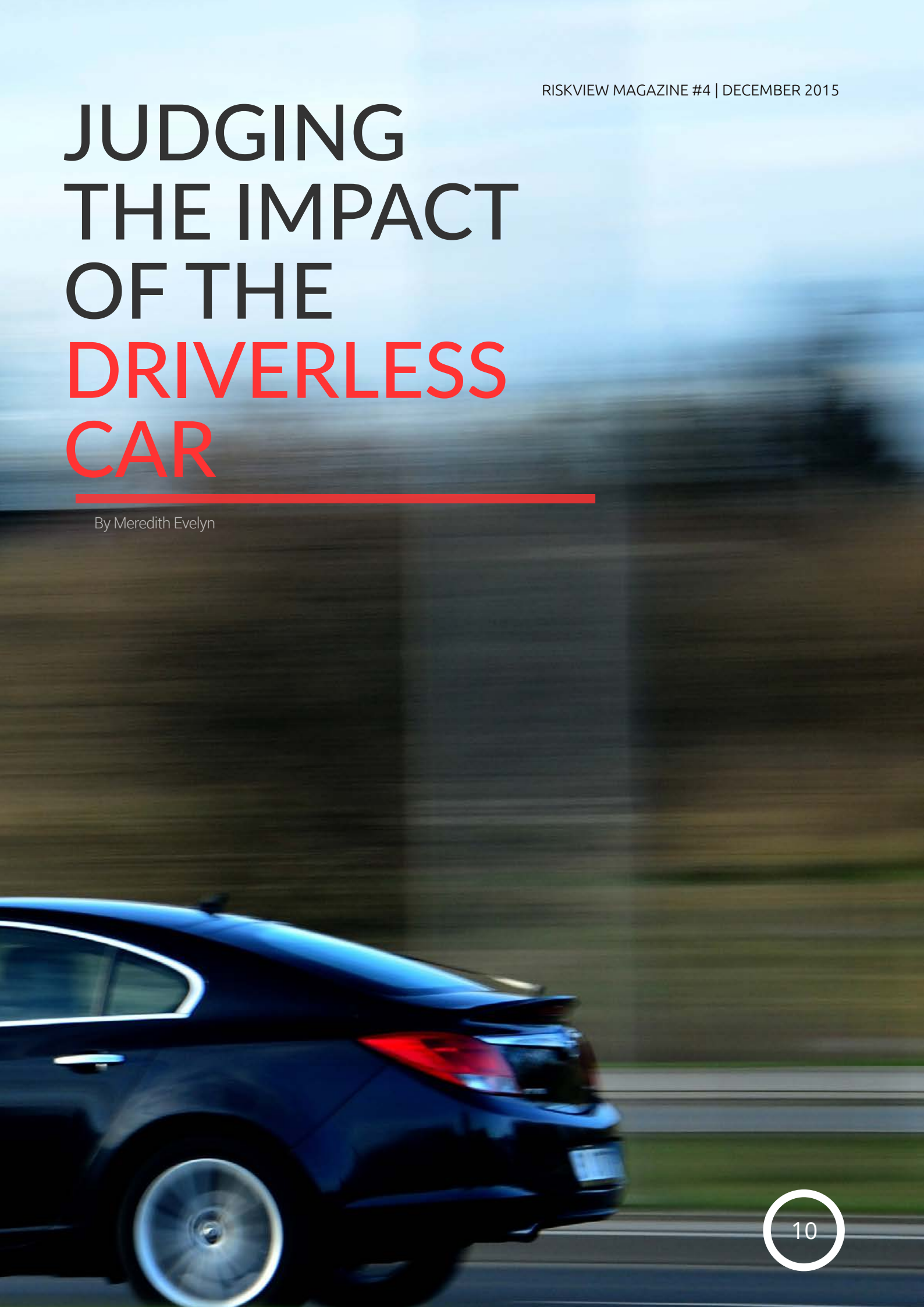
Respondents to the first surveys "consistently reported being more concerned about insider threats than external threats". But concerns about external threats increased when more than 4 million patient records were compromised in 2013 alone.

As a result, hospitals are changing their security tools. But while traditional security measures are still being relied upon, survey respondents seem to agree that existing security approaches "likely will not be successful in helping to defend from the cyber-attacks of tomorrow."

Worryingly, although HIMSS is now seeing a modest increase in the use of more advanced data security strategies and technologies, including intrusion prevention systems, data loss prevention tools, multi-factor authentication and Dark Web research, these are still "much less widespread."

JUDGING THE IMPACT OF THE DRIVERLESS CAR

By Meredith Evelyn



According to two insurance suppliers and an auto parts maker, driverless cars and the technology behind them could one day disrupt the way they do business.

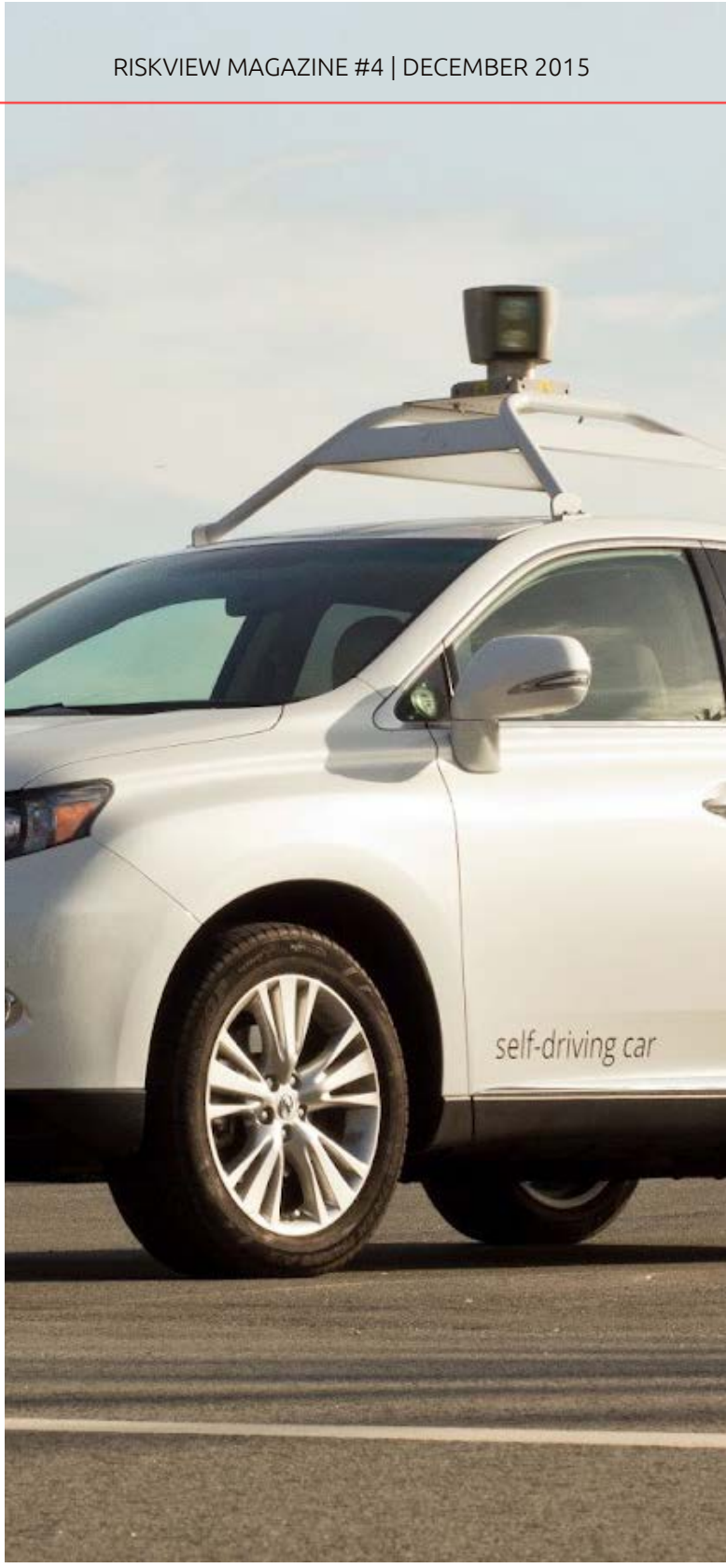
Cincinnati Financial Corp., an Ohio-based insurer generating nearly a quarter of its premiums from commercial and consumer auto policies, warned that its insurance liability forecasts could be flawed because of the "Disruption of the insurance market caused by technology innovations such as driverless cars that could decrease consumer demand for insurance products."

The cause for the concern is clear: according to the Insurance Information Institute, the industry took $107.4 billion in passenger car auto insurance premiums in 2013 alone.

However, insurers are not alone with their concerns over driverless cars. LKQ Corp., a Chicago-based auto-parts maker claimed, "If the number of vehicles involved in accidents declines or the number of cars being repaired declines, our business could suffer."

However, the impact of taking the driver out of the equation is difficult to predict. Jay Gelb, Barclay's insurance analyst, claims that insurers will have time to adapt as driverless cars become increasingly common and the Insurance Information Institute sees driverless cars as a natural result of advances in a variety of safety technologies. Like Gelb, the Institute believes that fewer accidents could make insurance cheaper, while at the same time, the more complex vehicles could be costlier to repair when crashes do occur.

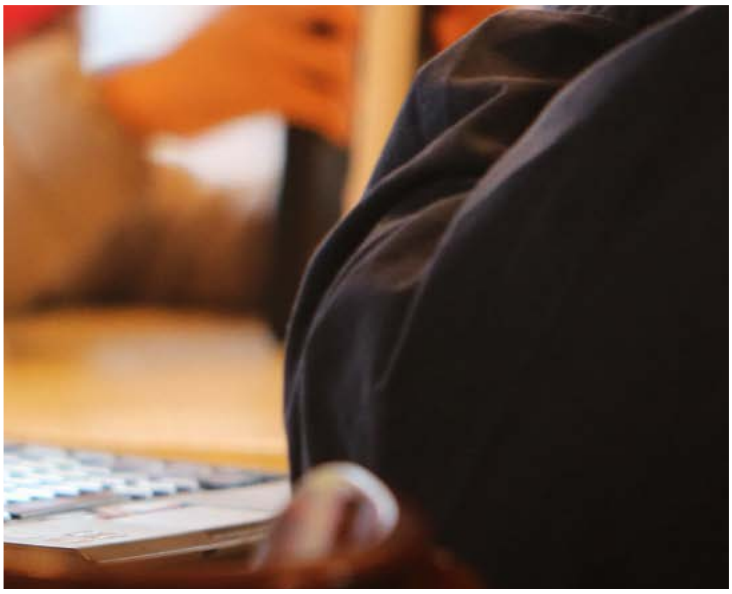
While driverless cars are still under development (Google Inc. has been testing its version for half a decade), they undoubtedly present a level of risk to the auto industry and its insurers. However, quantifying that risk is a complex exercise. This is why, for many companies, it is merely an opportunity to pick up on issues that may or may not affect their business in the future.



DIGITAL CHIEF OFFICER:

THE NEW KID ON THE MANAGEMENT BLOCK

By Willis Hudson



There are three words that carry an astonishing amount of weight and significance for every business in the world and those words are risk, governance and compliance. However, while many businesses have long recognized the need to have risk management, governance policies and compliance procedures in place, few would have foreseen the requirements that have arisen in the past five years ago for digital risk management.

Since our global usage of the web in all areas of life has started to dominate every area of the world, the risks posed to any business, whether local or multinational, has grown so fast that, according to Gartner, a third of large enterprises involved in any kind of digital business or activity will need a digital risk officer – or the equivalent – by 2017.

These days, global organizations need to deliver information locally because content and branding are often pitched at specific cultures and countries. For example, branding and content that is suitable for the UK market may not be suitable for that of the US or Asia Pacific. Added to this is the fact that regulation and compliance requirements vary from one country or region to another.

This means that senior executives in global and multinational organizations now need to manage and monitor their digital assets in line with the requirements of local legislative and regulatory bodies. As a result, one requirement of the DRO or risk management team is that it can easily report back to a local regulatory body or auditor and demonstrate the organization's compliance whenever they are asked to do so.

But DROs have other benefits, too. Many multinational companies have a tendency to produce duplicate or overlapping content but, with their ability to see across all functions, a DRO can ensure that assets purchased in one part of the company are available to other regions and areas of the business as well.

So, while there are many predictions about what the role of a DRO role might look like, what can businesses do now to prepare for this new hire?

Use your existing knowledge base

Most businesses, especially global organizations, will already employ expert staff (or consultants) such as lawyers, security executives, risk officers and senior executives. By combining the knowledge held by these people, an organization can gain a comprehensive overview of its digital assets and the legislative or regulatory requirements in each of its international locations.

Be local, not global

By auditing the businesses across every location and recording the different digital assets produced and stored the risk management team can start to gain a clear view of any challenges or areas for concern as well as flagging future challenges in a reliable risk management system.

Have a proactive approach

Being proactive means you will be able to prevent issues from arising rather than having to firefight them when they occur. This means putting in place robust risk management policies and procedures so you can detect, report on issues and address issues quickly and efficiently.

If you want to make compliance simple, you need to be proactive and make it easy for your entire staff to be actively engaged in the process. This means you need to keep things simple, be willing to continuously educate your employees and be prepared to foster a spirit of collaboration across the entire organization.

THE DIGITAL BOARDROOM:

A BRIDGE INTO A NEW WORLD

By Kendal Randy

Becoming a CEO is a huge achievement for most executives, not least because it is such a complex and demanding role. However, in the digital age, there is an additional requirement that needs to be added to the skill set of a CEO, and that is the ability to become a 'digital leader'.

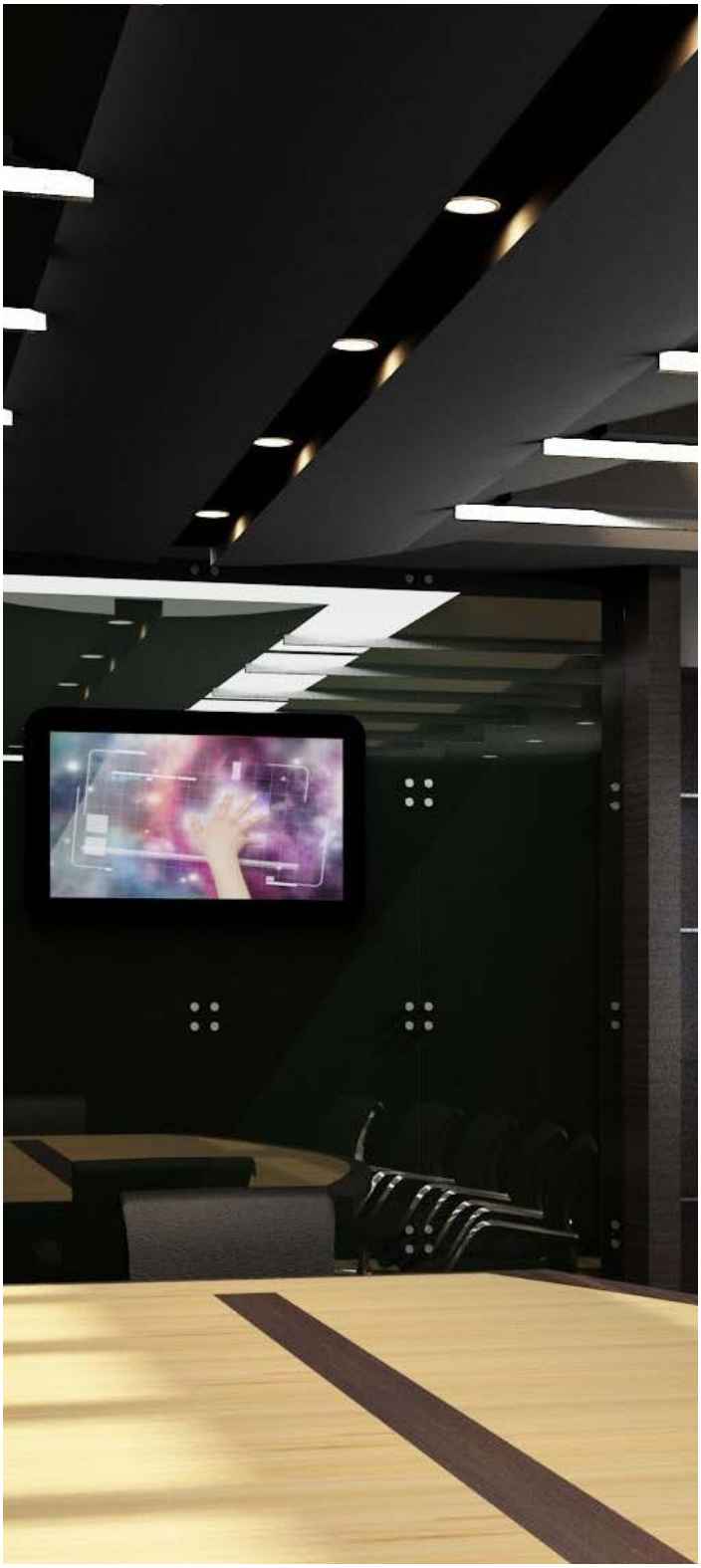
When digital transformations or succession plans are being discussed, the question often arises as to who among the board members is able to take up the role of digital leader. While the obvious choice appears to be the CIO, a Harvard Business Review Analytic Services survey recently revealed that most CEOs do not think their CIO is up to the job. This makes it clear that digital leadership goes beyond 'mere technology practice' within an organization.

What is more, the survey indicates that less than a quarter of business leaders believe their organization is adequately prepared for a future that is driven by digital technology. This knowledge and skills gap appears to be due in part to the lack of an appropriate forum where business leaders are able to learn about new technology from their IT leaders and the fact that IT leaders are too busy to pass on their knowledge.

Given this situation, the CMO (Chief Marketing Officer) could be considered a viable alternative to the CIO. However, a study conducted by Ovum and SapientNitro revealed that only 26 percent of CEOs planning transformative digital business projects were turning to their CMOs.

However, according to Alan Trefler, Founder and CEO of Pegasystems recently said in an interview with CXOtoday stated that, "When it comes to making the best successor to the CEO, it would be the Chief Customer Officer. Businesses need a customer-focused individual, who understands where the technology is going and also someone who can differentiate between the real capabilities they should be building or buying, and not give in to the hype."

David C Moschella, research director, CSC LEF noted in an article, "Global business leaders see the game-changing potential of emerging technologies, but many are unsure their firms possess the digital



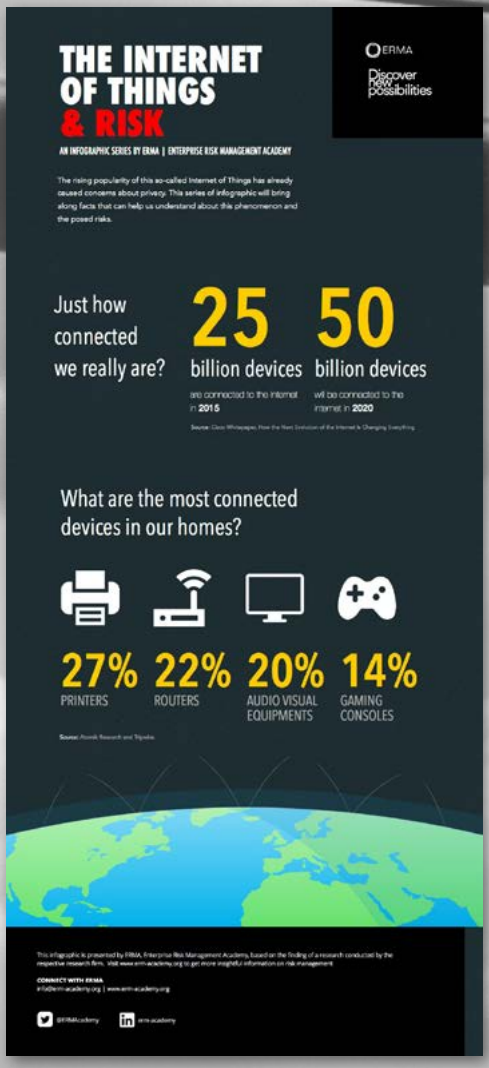
leadership necessary for these increasingly disruptive times."

Jake Sorofman, a Gartner analyst, puts the problem down to the lack of clarity and maturity of C-suites when it comes to understanding digital leadership. "Many organizations haven't grown up yet, and are stuck in a siloed legacy setup. They're used to looking outward at customers through different channels," he said.

The Red Hat report also revealed that companies that excelled in digital leadership were far more likely to have experienced revenue growth of at least 10 percent over the previous two years. Boards that delivered a clear vision and strategy for digital change and that had the people, processes and technology to execute that vision was significantly more likely to see revenue growth. 'Digital leaders' were considerably more confident in their company's ability to succeed in the digital age when compared to the rest.

Ultimately, experts believe that it does not matter which role takes on the responsibility of digital champion. Instead, it is more important that the board cooperates when making and implementing data-driven decisions and that it encourages an open culture throughout the business. Until that happens, the digital leadership gap will remain in place.

RISK MANAGEMENT INFOGRAPHIC



FIND OUT MORE:

https://erm-academy.org/publication/infographics

MANAGING THE EMERGENCE OF DIGITAL RISK IN THE NEXT 5 YEARS

By Meredith Evelyn

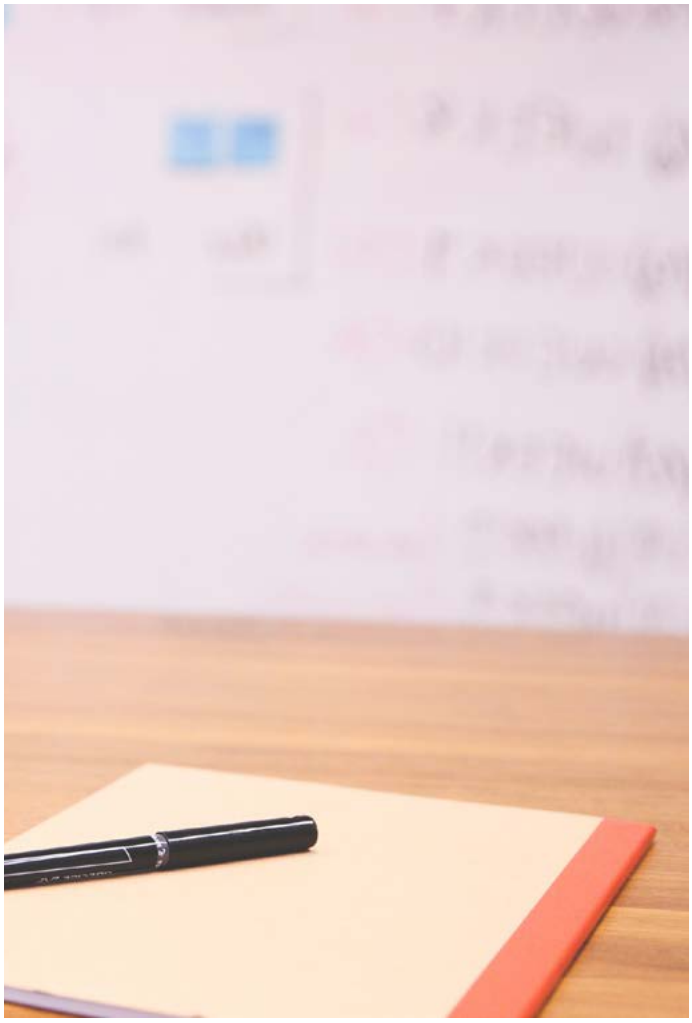
According to Gartner, a third of large enterprises engaged in digital business and activities will have a digital risk officer (DRO) role - or its equivalent- in place by 2017.

It also believed that 60 percent of digital businesses are likely to experience major service failures by 2020 as a result of the inability of their IT security teams to manage digital risks where new technologies and new uses of those technologies takes place. This means that digital risk management (DRM) is the next logical step in managing enterprise risk and security for digital businesses that are expanding the scope of technologies that need protection.

Paul Proctor, vice president and distinguished analyst at Gartner said that digital risk officers will require a mix of business acumen and understanding with sufficient technical knowledge to assess and make recommendations for appropriately addressing digital business risk. He goes on to say that, "Many traditional security officers will change their titles to digital risk and security officers, but without material change in their scope, mandate, and skills they will not fulfil this role in its entirety."

The scope and range of responsibilities in the DRO role will be different to that of a chief information security officer (CISO) so the CISO role will remain stable for now in many organizations. The DRO is likely to report to a senior executive outside of IT such as the chief risk officer, chief digital officer or the chief operating officer. DROs will manage risk at an executive level and across the business working directly with colleagues in the legal, privacy, compliance, digital marketing, digital sales and digital operations departments.

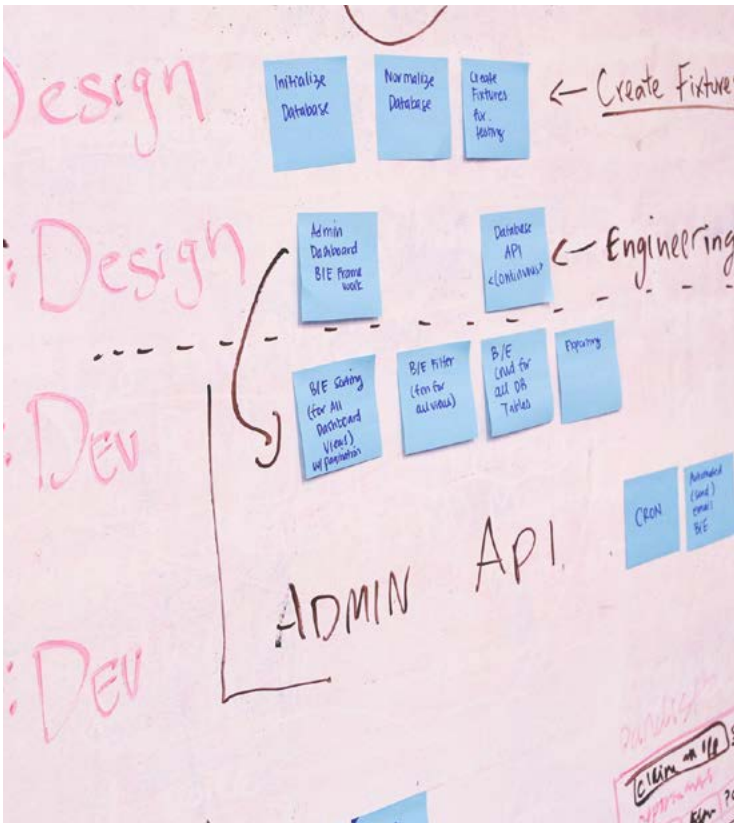
The IT security role will remain important and crucial to the business, but it is likely that many CISOs will morph into DROs as they begin to take responsibility for digital security and form effective partnerships with security teams that manage other forms of digital technology. Leaders in both IT security and physical security (as they become increasingly digital) are likely to continue with their existing responsibilities and report to the DRO.



In enterprises that have already appointed a chief risk officer the impact on IT and IT security operations of this new structure in digital risk governance and management is expected to be minimal. However, the impact on the culture of IT and IT security teams has the potential to be significant.

IT, OT, IoT and physical security all come together to form a new superset of technology. As such, this superset challenges the ability of existing organizational structures, the skill sets of its people and the tools it uses to assess, define and manage existing and new technology risks.

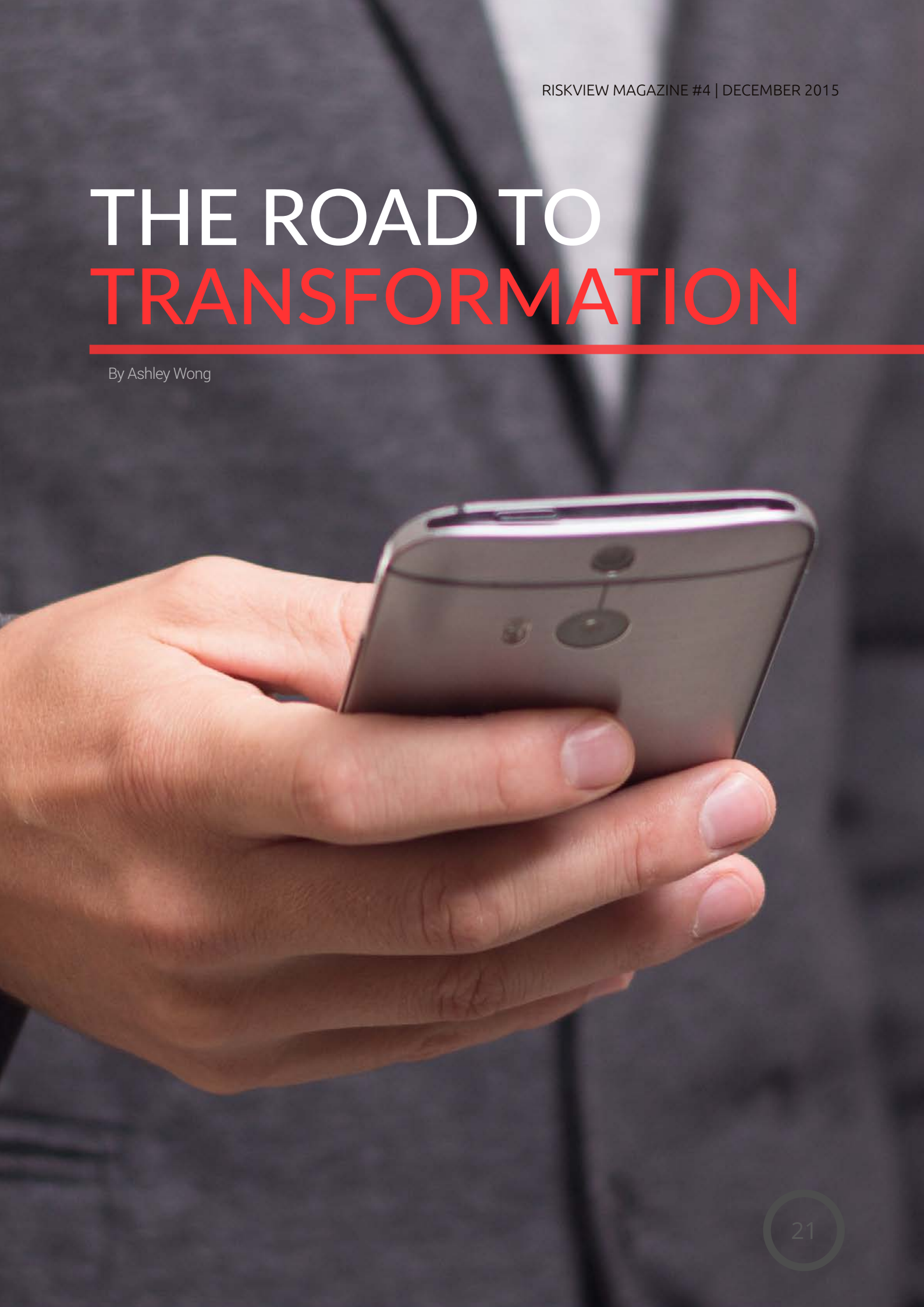
It is not viable to simply expand the role of the existing IT security team to include responsibility for risk in all Internet-connected technology. This is because both new and existing technologies that are managed separately to those of the IT organization demand skills and tools that are not part of the IT security team's competencies. Also, the culture in the teams responsible for managing these technologies is very different to that of the IT organization.

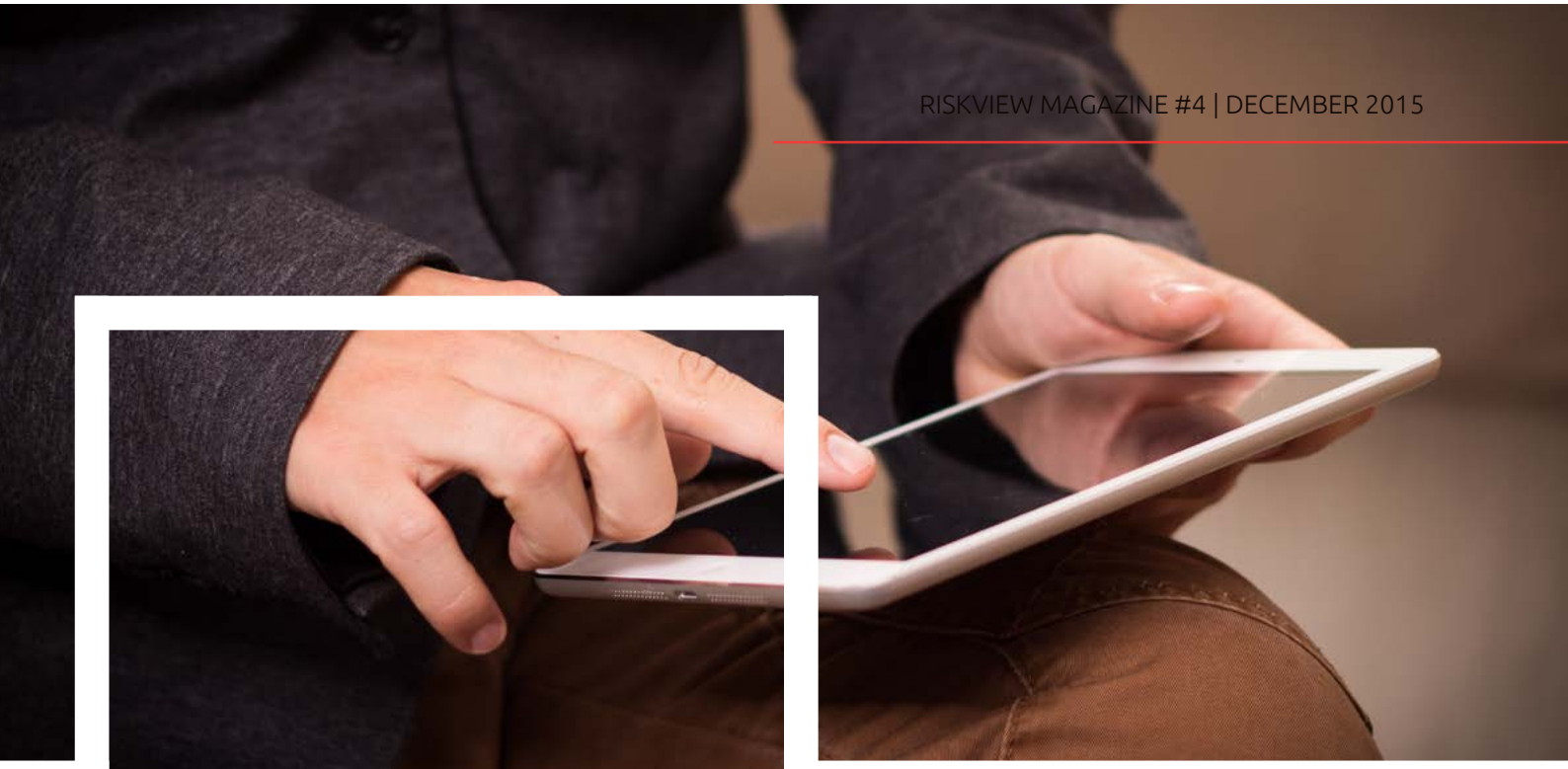


A unified and consistent approach to digital risk management has the potential to both save money and provide greater security for all business processes. To achieve this, digital risk management structures and roles need to be taken apart and reformed so that organizations are able to manage security and risk in a rapidly changing digital world.

THE ROAD TO TRANSFORMATION

By Ashley Wong





The world is changing fast and digital connectivity is, in one fell swoop, both bringing the world closer together and pushing it further apart. Good or bad, any business that does not take on board the challenges presented by digital transformation is going to get left behind.

What Is Digital Transformation?

Digital transformation is a phrase used to describe the changes that move an organization or business into the digital world. It is the point when the leaders of that organization decide to leave behind their existing operations and embrace the ever-changing business model brought about by technology. If you do not transform your business so it is ready for the digital world, you simply will not survive as a business. This is what you need to know before you start planning for digital transformation.

Decide what digital transformation means for your business

Implementing digital transformation is about more than just inserting technology into every area of your business. If you want to get it right, you need to think about what digital transformation means for your business. You need to:

- Digitalize your core client or business processes.
- Move your main business operations to a digital model.

There is no one-size-fits-all solution here, you will need to go through your own personal process and develop an understanding of which trends you need to follow.

Focus on your customer, not on the technology

Digitization that causes the most disruption Digitization that causes the most disruption to society, such as smartphones and wearable technology, has the most impact on consumers' lives, and it is the businesses that understand this best that thrive. Every business has to think about digital transformation and the power that creating and dealing with disruptions offers. If you

do not understand the significance or impact that technological disruptions cause, you cannot understand the changing needs of consumers or their shifting needs.

Plan your digital transformation in advance

Digital transformation is both an ongoing process a desirable end result in itself. Once you have started the process, you need to carry on because if you do not evolve you will be forced out of the marketplace. Digital transformation is no quick fix for a business, you need to think about the short term changes you need to make as well as your long-term goals. If you want to keep your business relevant, you will have to continue to implement digital solutions to keep your company moving forward into the digital era and not standing still or moving backwards.

You need to think about the business experience at every step. How can you use digital transformation to streamline in-house operations? How can you facilitate improved customer interactions using technology? It is these kinds of key question that will influence the direction of your digital transformation. You may decide to you adopt an integrated payment solution so customers can login to an online portal to pay their bills rather than paying by Direct Debit. It could be that you need to get active on social media and regularly post relevant content. So, any move into digital spaces will be part of your overall digital transformation.

In the long term, the digital experience is bound to shift so you need to build in change as part of your business processes. By constantly watching for changes in customer behavior, becoming aware of innovations and working to incorporate digital changes into the business you will be able to shift your company's focus away from old practices and over to a more digital-oriented future.

Once you have started your digital transformation, you need to keep going. Whether you run a local clothing shop or a billion dollar corporation, digital transformation needs to be an integral part of your core business, just like capital, overheads, and marketing.

TAKE-OVER ANXIETY:

DO WE NEED TO FEAR AI?

By Ashley Wong

Picture this: it is 2050 and a sentient machine is "living" in the US. It reads through the US constitution and, as a result, decides it wants to be able to vote. It also decides that it wants the right to procreate. These are fairly basic human rights and it believes it has a right to them given that it has human-level intelligence.

The question is, "Do you give it the right to vote or the right to procreate because you can't do both?" asks Ryan Calo, a law professor at the University of Washington. Professor Calo does not believe that human-level intelligence is going to be installed in our machines in the near future, but he does acknowledge that our relationship with sentient machines raises some interesting questions.

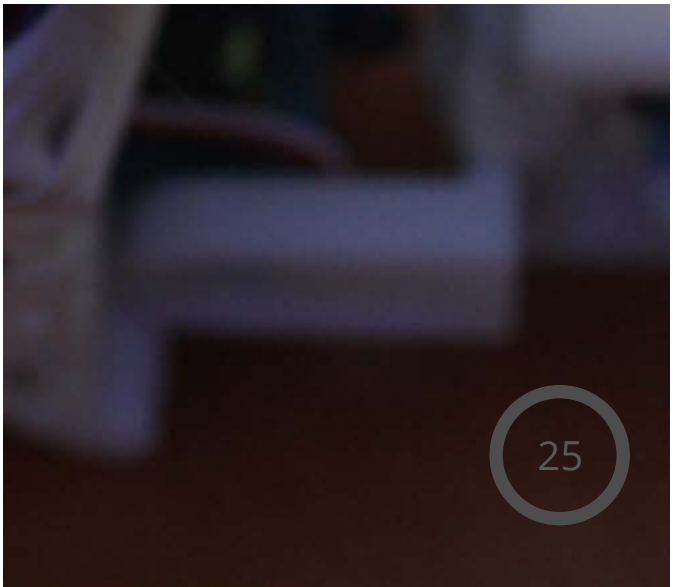
Recently, a robotic arm in a VW factory in Germany tragically crushed a young man who was also working there. Of course, industrial accidents happen all the time, but because it involved a robot, the law was a little uncertain (a human is unlikely to be able to sue a robot for damages).

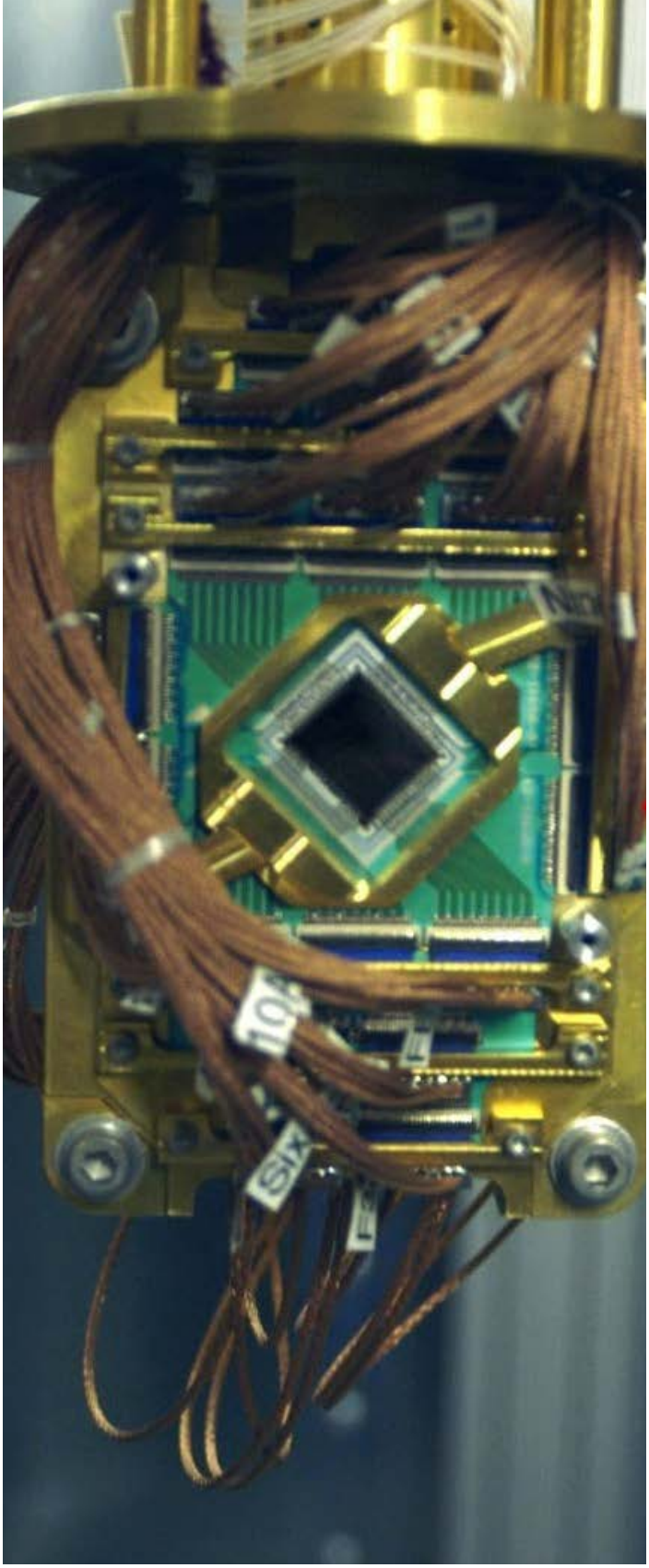
Many leading scientists and technologists are concerned about how the world is going to deal with the rise of artificial intelligence and many worries that it could present a threat to humanity. One such concerned person is Elon Musk, the founder of Tesla motors and the aerospace manufacturer, Space X. In fact, Musk describes the new technology as "summoning the demon" and claims that the super-intelligent computers that we are creating will treat us as little more than pets.

In his book, Humans Need Not Apply Jerry Kaplan also uses the pet analogy, painting a hellish picture of a human zoo run by "synthetic intelligence".

"Will they enslave us?" he asks, "Not really – more like farm us or keep us on a reserve, making life there so pleasant and convenient that there's little motivation to venture beyond its boundaries." He claims that our AI keepers will want to conserve us "just as we want to preserve chimps, whales, and other endangered creatures".

In reality, AI is still at it an early point in its development and it is difficult to guess where it will go. We are still a long way from being able to reproduce what takes place in the human brain using computer-based neural networks. As Andrew Ng, chief scientist at Chinese e-commerce site Baidu points out: "There's a big difference between intelligence and sentience. Our software is becoming more intelligent, but that does not imply it is about to become sentient."



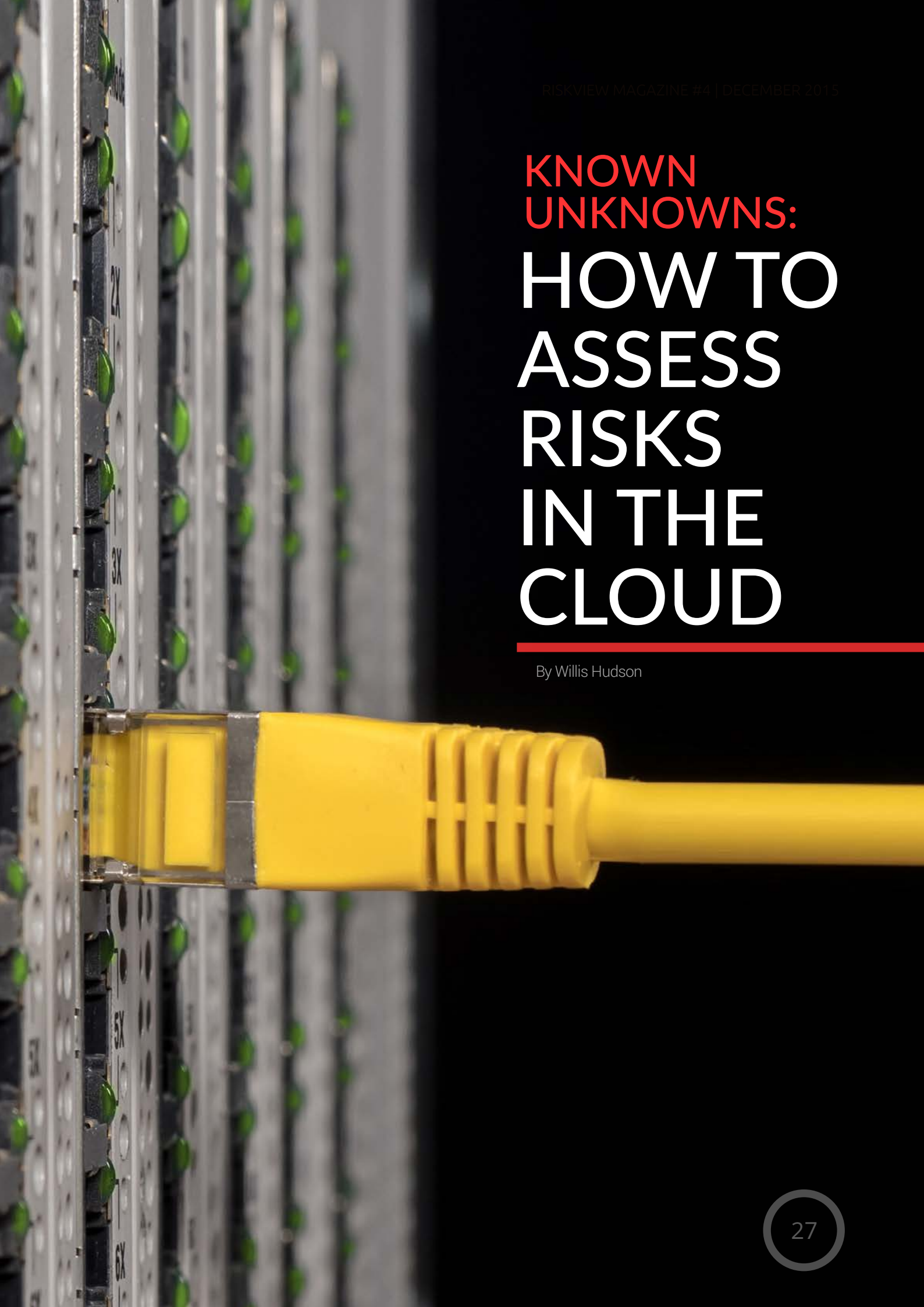


However, as author James Barrat points out in his book, Our Final Invention, the fact that AI is not sentient does not mean that it cannot be misused. "Advanced AI is a dual-use technology, like nuclear fission. Fission can illuminate cities or incinerate them. At advanced levels, AI will be even more dangerous than fission and it is already being weaponized in autonomous drones and battle robots."

Noel Sharkey, co-founder of the Campaign to Stop Killer Robots, believes we must set rules for bots of the future, partly because, "it is the ultimate human indignity to have a machine kill you," and partly because of the need to avoid robot wars and the disruption it would cause to global security.

In the absence of an agreed set of rules as to how robots should be allowed to behave, many refer to the three laws of robotics laid down by science fiction writer, Isaac Asimov in his short story "Runaround", published in 1942 as part of the fictional Handbook of Robotics, 56th edition 2058:

- A robot may not injure a human being or, through inaction, allow a human being to come to harm.
- A robot must obey the orders given to it by human beings, except where such orders would conflict with the first law.
- A robot must protect its own existence as long as such protection does not conflict with the first or second laws.



KNOWN UNKNOWNS: HOW TO ASSESS RISKS IN THE CLOUD

By Willis Hudson

You may well have had a few chuckles in the office over former U.S. Secretary of Defense Donald Rumsfeld's famous "unknown unknowns" statement, but anyone involved with computer security quickly understood what he was talking about. The truth is that we are constantly faced with three types of security risk: known knowns, known unknowns, and unknown unknowns.
Indeed, when it comes to the adoption of public cloud computing, it is the calculation of the additional risks posed by all the unknown unknowns that prevents companies from adopting cloud computing. For this reason, it is worth being aware of the five critical risks any business faces when using public cloud computing.

Cloud risk No. 1: Shared access

Multitenancy – where multiple and usually unrelated customers share the same computing resources – is one of the key tenets of public cloud computing. However, multitenancy presents a huge set of 'known unknown' risks. Not only is there a risk that private data is accidentally leaked to other tenants, there are other risks, too. These mainly arise from sharing resources because if the history of shared web servers is anything to go by, it is easy to see that multitenancy presents a long-term security problem.

Cloud risk No. 2: Virtual exploits

There are four main types of virtual exploit risks you need to be aware of: server host only, guest to guest, host to guest, and guest to host, but these are largely unknown and uncalculated in most risk models. All large cloud providers use virtualization, but unfortunately, virtualization contains all the risks posed by physical machines plus it has its own unique set of threats.

If you want to minimize the risk of virtual exploits, you need to ask your vendor what virtualization products or management tools they are using, how they are using it and what impact it has on their services.

Cloud risk No. 3: Authentication, authorization, and access control

Clearly, the authentication, authorization, and access control mechanisms used by cloud vendors are crucial to risk management. If you want to know what known and unknown risks you face you need to assess what facilities and processes your vendor uses. They may be unwilling to share this information, but you need to at least ask.

You need to find out whether data encryption is both used and enforced

and whether private keys are shared among tenants. You also need to find out how many people on the cloud vendor's team can see your data (and who they are), where your data is physically stored and how is it handled when it is no longer needed.

Cloud risk No. 4: Availability

When you use a public cloud provider, you lose control of redundancy and fault tolerance levels. This means that service interruptions and data loss become big risks (this is despite claims of high service levels by most cloud providers). To guard against these risks, your company needs to back up its shared cloud data or at least insist on a legal clause that gives it the right to claim damages if data is lost forever.

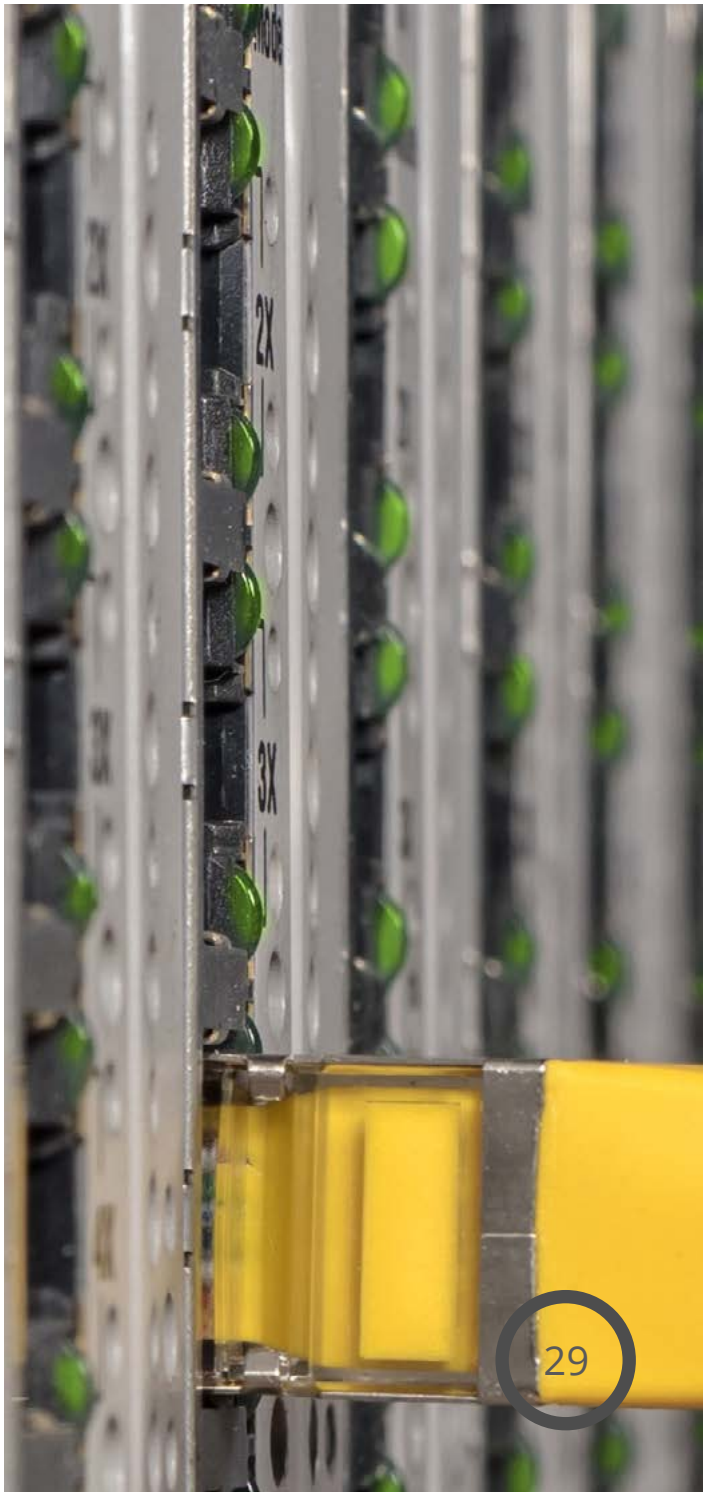
Cloud risk No. 5: Ownership

Most cloud customers are not aware of the fact that they do not own their data. Many public cloud providers have clauses in their contracts that explicitly state that the data stored belongs to the provider and not the customer.

Cloud vendors like to own the data on their cloud because it gives them more legal protection if something goes wrong. It also means they can mine their customers' data in order to create additional revenue opportunities for themselves. Make sure you know who owns your data and, if you are not the owner, what the cloud provider is permitted to do with it.

Cloud visibility

Even when cloud computing risks are known, their impact is difficult to assess with any accuracy. The best you can do is to ensure that you and your management team are aware of the known unknown risks your company faces. For this, you need as much information as you can get because it is only by asking difficult questions that can you begin to understand the risks posed by public cloud computing.



ERMA | ENTERPRISE RISK MANAGEMENT ACADEMY

RISKVIEW

To find out more about ERMA, visit www.erm-academy.org

CONNECT WITH ERMA
info@erm-academy.org | www.erm-academy.org

@ERMAcademy erm-academy