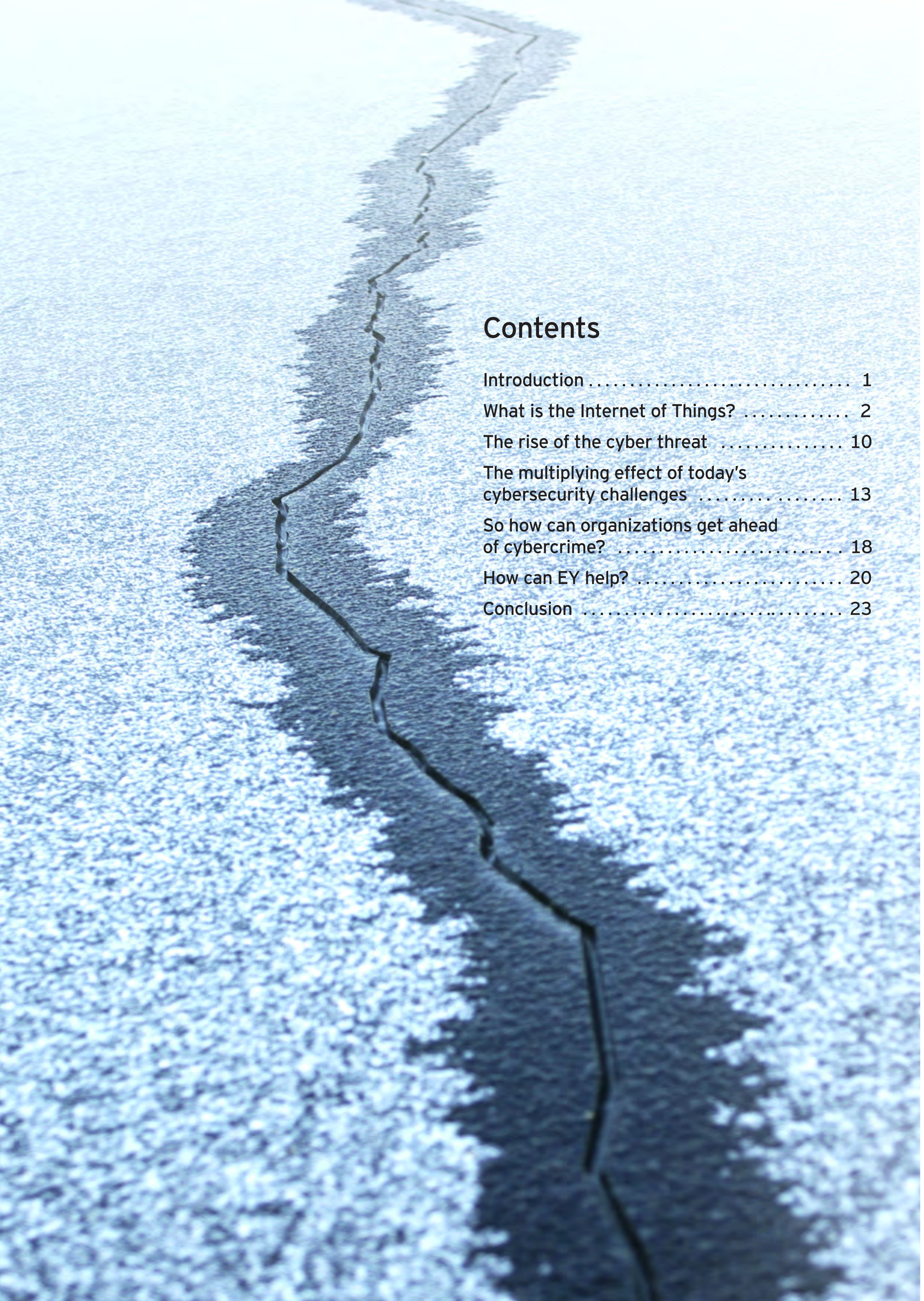
Insights on
governance, risk
and compliance

March 2015

Cybersecurity and the Internet of Things

Building a better
working world



Contents

Introduction 1
What is the Internet of Things? 2
The rise of the cyber threat 10
The multiplying effect of today's cybersecurity challenges 13
So how can organizations get ahead of cybercrime? 18
How can EY help? 20
Conclusion 23

The growth and spread of connected digital technology

Rapid technological change has resulted in many aspects of our lives being connected and affected by digital communications.

With billions of people connected to the internet today, and the number of connected devices to exceed 50 billion by the year 2020, the Internet of Things (IoT) represents a major transformation in a digital world that has the potential to affect everyone and every business.

IoT can be defined as physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community. The IoT will help to enable an environment with the flexibility to provide services of all sorts, ranging from home automation to smart retail/logistics, and from smart environmental monitoring to smart city services.

In a very short time, the IoT will have sensing, analytics and visualization tools, which can be accessed by anyone, anytime and anywhere in the world on a personal, community or a national level. The potential for it to enable any aspect of our lives is what is encouraging this idea to become established and flourish.

However, the real change is not that machines are talking to each other, but that people are talking more and more "through" machines — the IoT is actually the medium of interconnection for people — and because human communication is mediated by machines and is more and more indirect, there is a deeply rooted security problem with the possibility of impersonation, identity theft, hacking and, in general, cyber threats.

The IoT will increasingly rely on cloud computing, and smart devices with sensors built in, along with thousands (if not millions) of applications to support them. The problem is that the truly integrated environments needed to support this connected technology do not exist, and cloud computing is in need of serious improvement, especially in terms of security.

There is no single object that can be described as the IoT infrastructure — there are many disparate and uneven networks. Because of the increasing stresses on these networks, due to the demands of the data that needs to be supported, many technical areas will need to be redesigned. Additionally, the number of connected devices in circulation being used for the vast amount of interactions has created further challenges in data privacy, data protection, safety, governance and trust.

Taking all of these factors into consideration, we see both opportunities and challenges which require close attention and, in particular, the need for a comprehensive strategic approach to cybersecurity. This report highlights why being in a proactive position to anticipate and mitigate cyber threat is one of today's most important business objectives.

Mobility, digital business models, smart energy infrastructures and the adoption of cutting-edge technologies for transportation, consumer goods and services are transforming cybersecurity concerns. From the back office to the forefront of service quality and business development, security is now embedded in the core strategies of a leading business.

What is the Internet of Things?

The Internet of Things is the network of physical objects that contains embedded technologies to communicate and sense or interact with their internal states or the external environment.

The Internet of Things, Gartner IT. (n.d.). Retrieved from http://www.gartner.com/it-glossary/internet-of-things

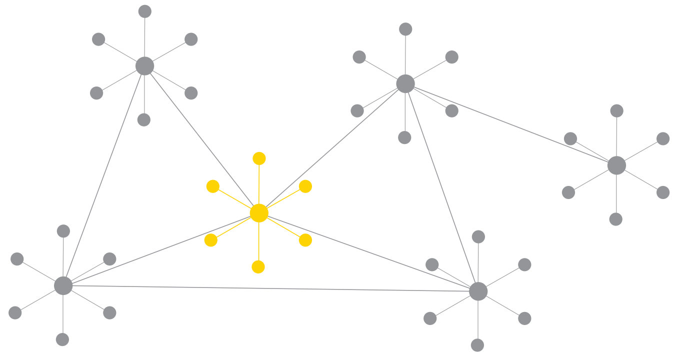
IoT is a future-facing development of the internet wherein objects and systems are embedded with sensors and computing power, with the intention of being able to communicate with each other. Although the original concept of IoT puts excessive emphasis on machine-to-machine communications, the real change underlying this is the diversification of people-to-people communications in an increasingly indirect way. Machines may eventually be able to communicate, but so far this phenomenon is neither universal nor covers all types of networks; even when machines can connect to each other, the fact is that they will remain as instruments of human communications.

The ever-increasing networking capabilities of machines and everyday devices used in the home, office equipment, mobile and wearable technologies, vehicles, entire factories and supply chains, and even urban infrastructure, open up a huge playing field of opportunities for business improvement and customer satisfaction.

Most IoT devices will use sensor-based technologies, in which the sensors will identify or measure any change in position, location, etc.; these sensors will transmit data to a particular device or server, which in turn will analyze the data to generate the "information" for the user. In business terms, the sensors will also act as data gatherers; cloud computing will be a platform for storing and analyzing the data, and Big Data analytics will convert this raw data to knowledge or insights.

Business models for the employment of IoT may vary for every organization, depending upon whether it is handling the core operations, manufacturing or the services/technologies. The retail and merchandizing sector, for example, could benefit from IoT innovations in the future: if a new customer enters a shoe shop, his or her shoe size could be measured by the measurement sensors; data could be sent over the cloud about availability of stock; the inventory could then be replenished based on real-time analytics and forecasted trends. Other examples for the same retail outlet could be parking sensors, motion sensors, environmental sensors, door sensors that measure footfall, and mobile payment services.

The network of people and things



The network of networks is the full-blown internet of people and things, where every machine-to-machine connection is actually mediated human interaction. These networks are simultaneously networks of collaboration, but also networks of opposition and threat: there is no "inside" or "outside" in this discontinuous, porous space.

IoT is not new

Although IoT is a hot topic today, it's not a new concept. The phrase "Internet of Things" was coined by Kevin Ashton in 1999; the concept was relatively simple, but powerful.

> If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so.
>
> *Kevin Ashton, "That 'Internet of Things' Thing," RFID Journal, July 22, 1999*

However, in 1999, there were still more questions than answers to IoT concepts:

- How do we connect everything on the planet?
- What type of wireless communications could be built into devices?
- What changes would be needed to support billions of new devices communicating constantly?
- What would power these devices?
- What must be developed to make the solutions cost-effective?

2015 – enabling technologies driving the successful growth of IoT

- The size and cost of wireless radios has dropped tremendously.
- IPv6 makes it possible to assign a communications address to billions of devices.
- Electronics companies are building Wi-Fi and cellular wireless connectivity into a wide range of devices (e.g., billions of wireless chips).
- Mobile data coverage has improved significantly with many networks offering broadband speeds.
- Battery technology has improved significantly, and solar recharging has been built into numerous devices.

The cloud provides a platform for IoT to flourish, however, there are still many challenges. With the plethora of data that they will hold, storage servers will have to be updated and secured all the time.

Now that we have entered the era of coordination of machine-to-machine, people-to-machine and people-to-people, connections have become much easier.

What opportunities does IoT offer?

IoT is leading change within the digital landscape – and it's fast becoming the must-have element of business technology. Some of the primary forces driving the adoption of IoT are:

- New business opportunities
  The web of connected devices, people and data will provide business opportunities to many sectors. Organizations will be able to use IoT data to gain a better understanding of their customers' requirements and can improve processes, such as supply chain/inventory coordination, investments and public safety.
- Potential for business revenue growth
  There are multiple untapped opportunities for economic impact by finding creative ways to deploy IoT technology to drive top-line revenue growth and value creation through expense reduction and by improving asset productivity.
- Improved decision-making
  Personal computing smart devices are on the rise, leading to wider choice, real-time updates, enhanced facilities, more accurate fact finding, etc. and thus leading to more informed decision-making.
- Cost reductions
  The costs of IoT components, such as cloud services, sensors, GPS devices and microchips, have fallen, meaning that the cost of IoT-linked devices is getting more affordable day by day.
- Safety and security
  With the help of cameras and sensors, there is the possibility to guard against, or avoid, physical threats, which might occur at the workplace or home. In time, even disaster management or recovery systems will get help from IoT.
- Improved citizen experience
  The citizen experience could improve considerably due to ease of access, ease of living and ease of communicating. Think of an example where a citizen can pay his or her taxes remotely, watch his or her parking space from the office, shut down or communicate with gadgets or machines at home, and even proactively monitor his or her health.
- Improved infrastructure.
  IoT could help to turn infrastructure into a living organism, especially when major megacities transform into "smart cities." Large population inflow in urban areas and depleted non-renewable energy sources are making resource management a challenge, but intelligent infrastructure and interconnected networks are starting to provide solutions with concepts, such as smart grid, smart waste management, smart traffic control, smart utilities and sustainable city. Microcomputer-enabled automated citizen services will also make future smart cities more secure and more efficient.

The ever-expanding IoT world

IoT is already integrated across several areas where technology adoption is accelerating. The key areas of leading IoT integration are:

Smart life

Innovative, state-of-the-art technology aims to make life simpler and safer for the consumer. Smart life includes:

- **Health care** – a new patient-centric model is emerging
- **Consumer and retail businesses** – the age of the empowered customer and co-creator
- **Banking convergence** – new models for banking and finance
- **Insurance** – moving from statistics to individual fact-based policies
- **Public services** – driving efficiency and convenience for governments and citizens

Smart mobility

Real-time route management and solutions aim to make travel more enjoyable and transportation more reliable. Smart mobility includes:

- **Autonomous driving and the connected car**
- **Urban mobility** – smart traffic management
- **Interurban mobility** – connecting across the transport networks
- **Fare management and payment solutions**
- **Distribution and logistics**
- **Fleet management**

Smart city

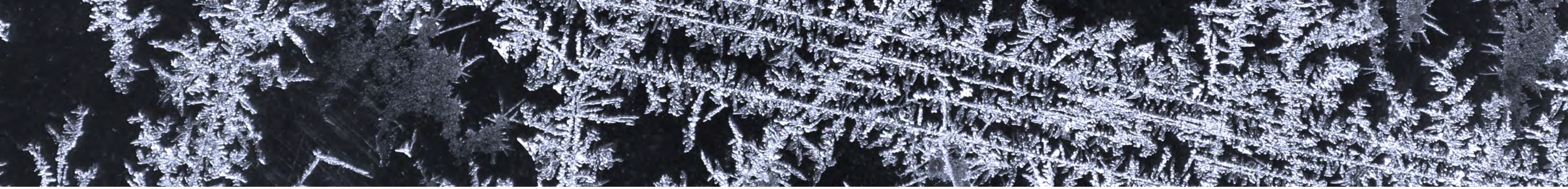
Innovations will aim to improve the quality of life in cities, encompassing security issues and energy resourcefulness. Smart city includes:

- **Smarter management of city infrastructure** – using Big Data analytics
- **Collaboration across multiple and disparate agencies** – using cloud technologies
- **Real-time data collection, enabling quick response** – using mobile technologies
- **Enhanced security** – improved public safety and law enforcement, and more efficient emergency response
- **Better city planning** – improved schematics, project management and delivery
- **Networked utilities** – smart metering and grid management
- **Building developments** – more automation, and better management and security

Smart manufacturing

Factory and logistics solutions will be created specifically to optimize processes, controls and quality. Smart manufacturing includes:

- **Machine learning** – intelligent, automated decision-making
- **Machine communications** - more interaction and collaboration
- **Networking** – networked control and management of manufacturing equipment
- **Optimized processes** – rapid prototyping and manufacturing, improved processes and more efficient supply chain operations
- **Proactive asset management** – via preventive diagnostics and maintenance
- **Better infrastructure integration** – overcoming the interface standards conundrum



Economic benefits of IoT

Just like any other market where demand is directly proportional to the supply, IoT also has a similar economy, with the potential for trillions of dollars of value waiting to be created for both the end users and public and private sector enterprises.

With the growth of IoT, many IT technologies will grow in parallel. For example, cloud computing and Big Data markets give IoT a platform from which to grow and evolve.

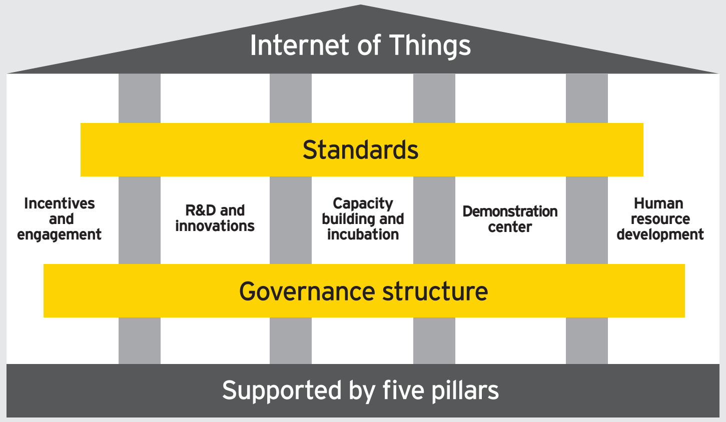
IoT will offer opportunities for companies which are manufacturing IoT goods, and also for those companies which are providing services related to IoT. The manufacturers of smart devices, sensors or actuators, and the application developers, marketing strategists, analytic companies and internet service providers (ISPs) will all profit from the evolution of IoT. According to industry estimates, machine-to-machine (M2M) communications alone will generate approximately US$900 billion in revenues by 2020.

The market is currently focusing on the vertical domains of IoT since it is in relatively early phases of development. But IoT cannot be treated as a single thing, or single platform, or even a single technology. In order to achieve the expected rapid growth from IoT opportunities, more focus needs to be put on interfaces, platforms, mobile applications and common/dominant standards.

IoT policy framework: developing economies' perspective

India is planning to invest approximately US$11 billion for developing 100 smart cities. A draft policy framework document of IoT was released in October 2014 by the Indian government, which proposed the following model.

The two horizontal pillars are standards and governance structure, which are defined as the two governing forces. The future of IoT can be said to be dependent on these two as the former will define the standards for communication, safety, privacy and security, whereas the latter will define the formation, control and power of the government agencies.


Internet of Things
Standards
Incentives and engagement
R&D and innovations
Capacity building and incubation
Demonstration center
Human resource development
Governance structure
Supported by five pillars

Source: Department of Electronics and Information Technology, Government of India

IoT will affect different business sectors in different ways

Key sectors , such as health care, education, financial, retail, communications, hospitality, industry, transportation and agriculture, are already enriched by internet-based technology, and further advancements will make other key economic sectors part of the digital connectivity landscape.

In the past decade, the **health care** sector has been one of the biggest beneficiaries from IoT. Although by no means universal, future solutions may become available such as:

- Personal information that could tell medics not only about individuals' medical history, but also about potential diseases
- Sensors and microcomputers fitted in the human body that could monitor health conditions and even alarm emergency services in case of any distress
  - Similar technology could make living ambience more suitable to an individual's medical requirements
- Highly automated devices and processes could help to increase critical treatments efficiency with a limited human interface

IoT in the **education** sector has already started to make the conventional education system more automated – interactive smart classrooms are helping students learn and participate more, whilst automatic attendance and various student tracking systems could help to make schools more secure. Internet-enabled remote classrooms will be a milestone for developing countries, making deep penetration in areas where setting up a traditional school infrastructure is not possible.

Internet-enabled **manufacturing and industrial** units are giving differentiating results, making them safer and more efficient through automated process controls. Plant and energy optimization, health and safety control and security management are now increasingly being provided by advanced sensors, networked with sophisticated microcomputers.

Financial services are already leveraging the internet for many of their services. Exponential improvement in digital infrastructure and the next generation of IoT-enabled products could further lead the growth of the financial sector, with innovations, such as smart wearable and smart monitoring devices, helping customers to keep better track of their money and investments.

Telcos could face a surge in data usage due to IoT-enabled devices, thus raising their ARPU (average revenue per user), while on the other hand, they will also have to deal with some concerns, such as privacy and infrastructure security.

According to industry estimates, machine-to-machine communications alone will generate approximately US$900 billion in revenues by 2020.

The connected car

The connected car is just one way in which IoT is going to impact our lives significantly (and very visibly) in the near future. Here, we address the security requirements of the connected car platform and its environment, but the approach is relevant for all IoT-related innovations.

Connected car security

Similar to the grid (e.g., smart meter) and other mobile and internet-connected systems, the connected car ecosystem should be viewed as a "network of networks" (or a system of systems). The connected car is just one more link (albeit the "newest" one and the most likely to be the focus of attention) in a much wider and complex network.

When taking this point of view, we see the need to shift the emphasis from the connected car as a cleanly defined system, with clear boundaries and input/output points, and take instead as our object of protection the networks themselves, i.e., the interactions between the users/owners of the vehicles and the numerous other actors in the ecosystem. Security becomes then the security of those interactions and is not limited to the car as a "thing."

It is vital to understand the uneven character of digital and network technologies. So, for example, while some studies predict that 70-90% of the motor vehicles may be connected by year 2020, other data indicates that 80% of this connectivity will be very limited (e.g., only through the mobile phone and only for entertainment and "content services"). There won't be universal connections across brands and much less for the entire functionality of the cars for the foreseeable future.

Fundamental change

Because the connected car "lives" in the network, security is not a matter of closing doors and encrypting data; security means managing shared data and a more complex network of participants. Opening the on-board network to the internet means that legacy networks and applications become exposed and the "attack surface" increases as the business model expands to new areas, partners and user types.

The target of protection, the object of security, becomes the network of networks, not the individual car, and all cybersecurity measures and technologies need to be aligned with this goal in mind. Security requirements must be addressed at the application/channel level, but in some cases, this blocks the ability of the auto manufacturer to have a coherent strategy.

When considering connected car initiatives, businesses need to establish a solid legal understanding of data ownership and data protection policies. Only on that basis will it be possible to design agile and secure services that will enhance business operations. So far, in Europe and the rest of the world, issues around data protection do not have a uniform answer yet, and this area requires more work from the angle of information security.

Connected car networks need standard protection measures as security gateways (policy enforcement point) and firewalls (to block DOS and protocol attacks), but this also requires several layers or zones (based on assurance levels and access controls), where each layer implements a security policy. Data ownership and classification must underpin security levels (separate access routes and roles, data path segregation, etc.).

Connecting to multiple trusted and untrusted networks requires a new trust model, but closing the trust gap between the manufacturer and the car owner and between the manufacturer and commercial partners (providers) means balancing risk and trust considerations to create a win-win situation for everyone.

After-sales market and relationship development can be enabled by a security model with clear opt-in and data sharing rules, for example:

- New functions being adopted by the business (e.g., operating incrementally in several roles, including as service providers)
- Business operates in an extended "value chain" with no borders
- New partners are introduced (content providers, etc.)
- Building new relationships with customers (e.g., enabling customers to select products and services online)
- Extending information networks and technologies (e.g., linking transport and distribution networks; or establishing connections with vehicles for service, maintenance and marketing purposes)
- Linking previously physically isolated systems under collaboration networks and enabling remote access (e.g., virtual desktops and software as a service)

The connected car is the focus of EY's *Inside Telecommunications* newsletter, issue 15, 2014: www.ey.com/insidetelco15

The rise of the cyber threat

70%
of the most commonly used IoT devices contain vulnerabilities.

HP study reveals 70% of Internet of Things devices vulnerable to attack. (n.d.). Retrieved from http://h30499.www3.hp.com/t5/Fortify-Application-Security/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284#.VHMpw4uUfVc

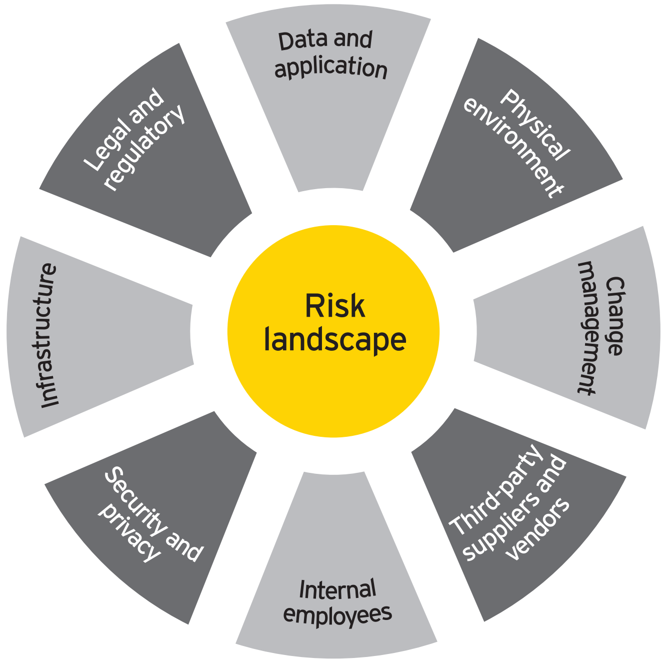
While the IoT is entering daily life more and more, security risks pertaining to IoT are growing and are changing rapidly. In today's world of "always on" technology and not enough security awareness on the part of users, cyber attacks are no longer a matter of "if" but "when."

Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information – they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property.

Every day, their attacks become more sophisticated and harder to defeat. Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time; we can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of this threat fade, new sources will emerge to take their place. Despite this uncertainty – in fact, because of it – we need to be clear about the type of security controls needed.

Effective cybersecurity is increasingly complex to deliver. The traditional organizational perimeter is eroding and existing security defenses are coming under increasing pressure. Point solutions, in particular antivirus software, IDS, IPS, patching and encryption, remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

56%
of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.**



Cyber attacks have transformed the risk landscape

It's important to remember that cybersecurity is a business-wide issue and not just a technology risk. Since many opportunities for IoT will arise through technological integration and collaboration, which will continue to increase in complexity – this complexity breeds risk.

Traditional proven risk management models have their origins and wisdom still focused in a world where the organization owns and possesses most, if not all, of the data assets flowing through the systems. The increasing use of the internet and mobile working means that the boundary of the enterprise is disappearing: and as a result, the risk landscape also becomes unbounded.

With most of today's business being done outside the organization's defensive fence, it is vital for organizations to be able to communicate with their business partners – and to do this they must create "holes" in the fence. As a result, a cybersecurity system should also include the organization's broader network, including clients, customers, suppliers/vendors, collaborators, business partners and even their alumni – together called the "business ecosystem."

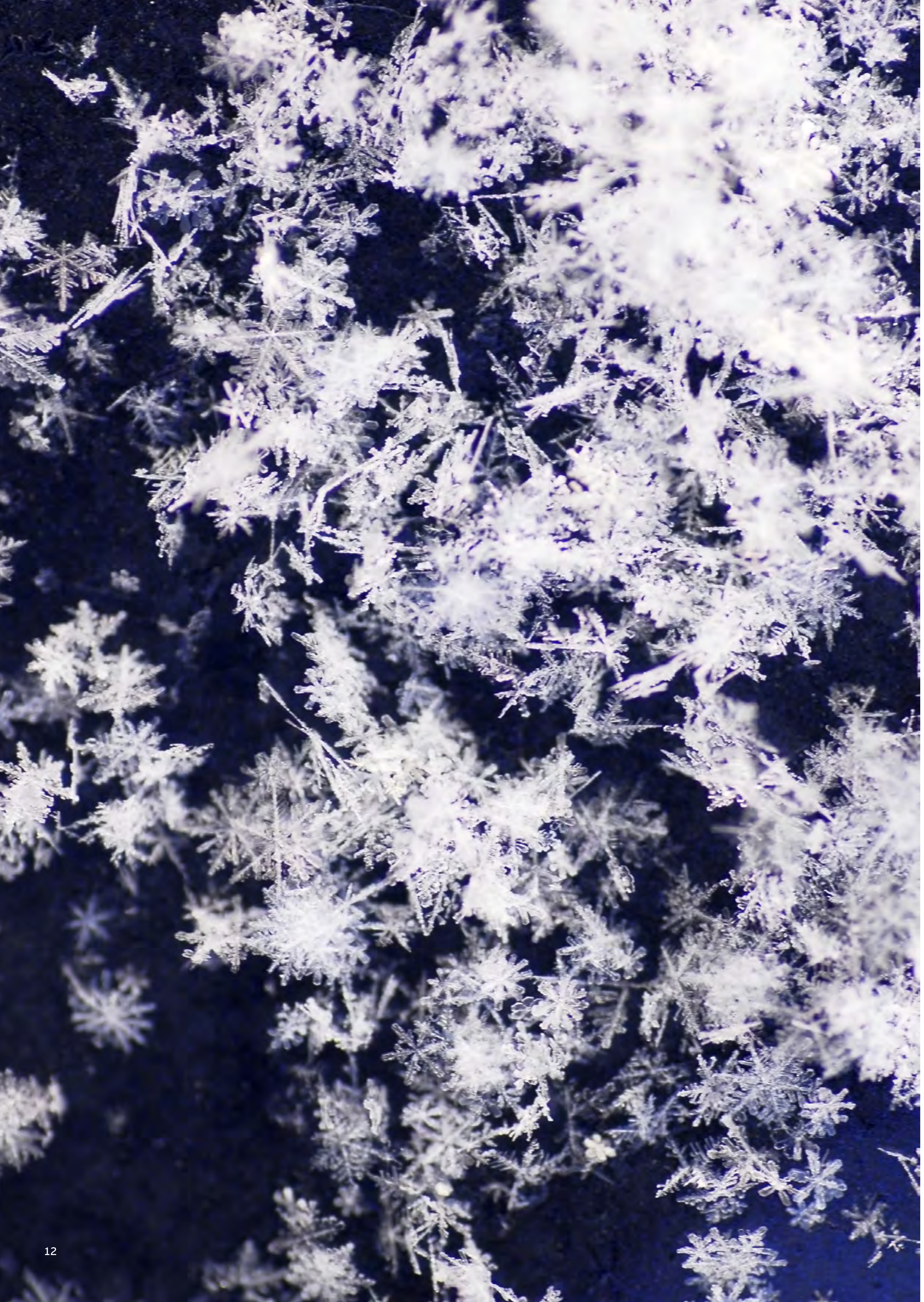
A standard approach to risk management assumes that the trust boundary is already defined. What is missing in the risk-focused and techno-centric approach is everything related to the management of trust, i.e., the new functions and processes, and the new policies and structures required to expand the risk boundary.

An extended ecosystem is governed and managed by various actors with individual policies and assurance requirements; and these actors sometimes have very different interests and business objectives within the collaboration. It is therefore necessary to adjust the organization's normal risk focus to take this into consideration.

For an organization to be able to effectively manage the risks in its ecosystem, it needs to clearly define the limits of that ecosystem. It also needs to decide what it is willing to manage within those boundaries: is it just the risks faced by groups that are one step from the organization itself (e.g., suppliers), or should the organization also try to influence the mitigation of risks faced by groups that are two steps from the center (e.g., the suppliers of suppliers)?

The security of the "thing" is only as secure as the network in which it resides: this includes the people, processes and technologies involved in its development and delivery.

**Survey statistics refer to EY's 17th Global Information Security Survey 2014, which captures the responses of 1,825 C-suite leaders and information security and IT executives/managers, representing most of the world's largest and most-recognized global companies. Responses were received from 60 countries and across nearly all industries. For further information, please access: www.ey.com/GISS2014.



The multiplying effect of today's cybersecurity challenges

The interconnectivity of people, devices and organizations in today's digital world, opens up a whole new playing field of vulnerabilities — access points where the cyber criminals can get in. The overall risk "landscape" of the organization is only a part of a potentially contradictory and opaque universe of actual and potential threats that all too often come from completely unexpected and unforeseen threat actors, which can have an escalating effect.

The speed of change

In this post-economic-crisis world, businesses move fast. New product launches, mergers, acquisitions, market expansion, and introductions of new technology are all on the rise: these changes invariably have a complicating impact on the strength and breadth of an organization's cybersecurity, and its ability to keep pace.

A network of networks

The adoption of mobile computing has resulted in blurring organizational boundaries, with IT getting closer to the user and further from the organization. The use of the internet via smartphones and tablets (in combination with bring-your-own-device strategies by employers) has made an organization's data accessible everywhere and at any time.

Inevitably, one vulnerable device can lead to other vulnerable devices, and it is almost impossible to patch all the vulnerabilities for all the devices. For the cyber criminals, it won't be hard to find a target for their attack. The market of vulnerability (the underground black market selling botnets, zero days, rootkits, etc.) will be vast and so would be the number of victims. It is easier for an attacker to plant a "Trojan" in a phone, if the phone is connected to the computer which has already been compromised. With even more devices connected, it will be even easier for a cyber criminal to get into your attack vector.

Machines or devices will be help people in performing most of their tasks, but consider the scenario when somebody gets a peep into any of our smart devices. In a recent event, the hackers hacked into a baby monitor and after having a good look around at their way in and way out through the camera, they broke into the house.

Infrastructure

Finding loopholes to enter any network will be easier for any attacker since there will be so many ways to attack. Traditionally closed operating technology systems have increasingly been given IP addresses that can be accessed externally, so that cyber threats are making their way out of the back office systems and into critical infrastructures, such as power generation and transportation systems and other automation systems.

Cloud computing

Cloud computing has been a prerequisite for IoT from the very early days of its evolution. The cloud provides a platform for IoT to flourish, however, there are still many challenges which we face today when it comes to cloud security or data security in the cloud. Organizations are often discovering too late that their cloud provider's standards of security may not correspond to their own. The recent events of "CelebGate" and Amazon's IAAS compromise are the live examples of such flaws. These are the incidents which have led the critics to call these services as single point of hack, instead of a single point of storage.

With Big Data also coming into picture, there will be an enormous amount of data produced for the service providers as well. With the plethora of data that they will have, the storage servers will have to be updated and secured all the time. There will be an increase in risks for communication links too, since the sensors and devices will be communicating sensitive personal information all the time on the channels.

With our data stored on such cloud services, there is also a risk of increase in spam as the cloud servers are virtually moved from one geographic location to another in a matter of minutes, depending upon the requirement. Hence, there is no IP-specific blockage possible for any spam.

Application risk

Apps have accelerated the integration of mobile devices within our daily lives. From mapping apps, to social networking, to productivity tools, to games, apps have largely driven the smartphone revolution and have made it as significant and as far-reaching as it is today. While apps demonstrate utility that is seemingly bound only by developer imagination, it also increases the risk of supporting BYOD devices in a corporate environment.

As the organization enables employees to bring their own devices, the need for using the same devices to access work-related data inevitably presents itself. This presents mainly two security risks:

- Malicious apps (malware): the increase in the number of apps on the device increases the likelihood that some may contain malicious code or security holes
- App vulnerabilities: apps developed or deployed by the organization to enable access to corporate data may contain security weaknesses

253 billion

The estimated number of free apps is projected to reach 253 billion by 2017.*

* Retrieved from http://www.statista.com/statistics/241587/number-of-free-mobile-app-downloads-worldwide

Growing use of mobile devices

Smart phones have already become an integral part of our lives; we rely on them to hold significant information, such as our home address, credit card details, personal photos/videos, e-mail accounts, official documents, contact numbers and messages. The information stored on our devices will include the places that we visit frequently and a "pattern" that uniquely identifies us, so anyone who can hack into any of these devices can get into our lives very easily.

The loss of a single smart device not only means the loss of information, but increasingly it also leads to a loss of identity (identity theft).The internet knows no monopoly and hence all devices cannot have the same firmware or software running on them. Hardware from different companies might not support each other and thus it might lead to interoperability issues of devices.

The increase in the number of devices can also be a problem as the vulnerabilities that they are associated with will spread very rapidly. With thousands of vendors across the globe, it will be very difficult for the network engineers to patch these vulnerabilities, especially with thousands of new patches to update daily — IoT network engineers will now have tenfold devices communicating to their servers outside the network.

Organized cyber criminals will be able to sell hardware with Trojans or backdoors already installed in them, and with the help of these vulnerabilities, they will hunt other victims and make a botnet out of it. These devices, scattered all around the world, will be perfect for a DDOS attack on any of the servers, since sensors don't have antiviruses.

The "bring your own device" employer

With most employees now owning mobile devices, organizations have been exploiting the fact that their employees increasingly want to use their own personal mobile devices to conduct work (often alongside corporate-provided devices), or if an organization requires its employees to do so, it is a cheaper alternative than providing the organization's own. Many organizations are reaching out to corporate IT to support this.

However, BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership. A holistic and methodical approach should be used to define this risk and help to ensure that controls exist to maintain both the security and usability of the devices in the enterprise.

Bandwidth consumption

Thousands of sensors, or actuators, trying to communicate to a single server will create a flood of data traffic which can bring down the server. Additionally, most of the sensors use an unencrypted link to communicate, and hence, there is a possibility of lag in the security.

The bandwidth consumption from billions of devices will put a strain on the spectrum of other wireless communications, which also operate on the megahertz frequencies like radio, television, emergency services, etc. However, companies have started taking this seriously; as a result, Qualcomm has launched its low power Wi-Fi connectivity platform for IoT.

Governance and compliance issues

Increasing privacy legislation is a trend that likely will continue in the near future. As organizations design IoT security controls, these may interfere with personal expectations of privacy. A well-formed IoT policy should include defined, clear expectations on privacy-impacting procedures, bearing in mind that legislation may differ in certain geographical regions.

Privacy and data protection

All smart devices hold information about their users, ranging from their diet plan to where they work; smart devices will include personal life details and often even banking details. All IoT devices gather accurate data from the real world, which is excellent from an analytics prospective, but a user might not be comfortable with sharing that data with a third party — even if not all the data is confidential or sensitive.

With the surfeit of data from billions of devices, there will be plenty of opportunities for analytical organizations; these analytical frameworks will be able to quantify the business environment around the users but, at the same time, the monetization of this data can lead to privacy issues. The question is: do we feel comfortable in sharing our data with people we are not even aware of? Doesn't it feel like a breach into our privacy? Should there be better transparency on how data is stored, used and transported?

According to OWASP (open source web application security project), some of the top privacy risks also contain web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer.

In the application of data protection and privacy law, as well as the access control model, one of the main objectives is that aggregated customer data should not enable anti-competitive, illegal or discriminatory uses. Collection of personal information must be always formally justified (including an impact assessment) and restricted to the minimum necessary for business purposes. According to established regulations, data should be retained for as short a time as possible, strictly to support business operations.

If the organization is collecting personal data, the purpose, expiration, security, etc., of the data collected must be clearly stated in the information security policy. The organization also must undertake a risk assessment of the risks associated with the processing.

If data is processed by a third party (i.e., if the organization utilizes a cloud email provider), it is important that the data be protected by a data processing agreement with the third party. With the transference of data, the responsibility of protecting that data also should be transferred and compliance verified. However, it is interesting to note that most cloud vendors currently either don't have a privacy policy or have non-transparent policies, which makes users a little uncomfortable about relying on them.

Breach investigation and notification

Following the impact of highly publicized cyber attacks, new and future legislation is proposed on cybersecurity, with fines being levied on companies who do not protect consumer data, and mandatory actions are being introduced around data breach notification. Organizations should prepare for this legislation by keeping an active inventory of devices, the data on them and the security controls in place to protect that data.

Some of the top privacy risks are web application vulnerabilities, operator-side data leakage, insufficient data breach response, data sharing with third parties, and insecure data transfer.*

* OWASP, Top 10 Privacy Risks Project. (n.d.). Retrieved from https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

Cybersecurity and smart energy grids

A step change in the evolution of the energy ecosystem

Smart meters and grid infrastructures will generate considerable benefits across the energy lifecycle – from generation through to distribution and consumption. This includes:

- The ability to match supply and demand
- Reduced cost through remote administration of devices
- Better informed consumers through real-time availability of granular energy consumption data

However, if the transition to smart and grid energy management is not developed correctly, there are significant cybersecurity threats to which organizations operating in this space will be exposed.

Smart meter and smart grid complexity

The smart meter infrastructure depends on a wide complex of networked systems, with different technologies and security levels, creating an environment which is difficult to assess from the point of view of data protection and cyber threat management.

Enterprise networks of energy suppliers, each with their own ecosystem, must be connected to the smart meter and grid infrastructure, generating requirements for standardization and regulation of the security mechanisms and processes. The complexity of this environment is not transparent for the general public.

Agreed legitimate uses of stored data need to be complemented with mechanisms to minimize the risk of unauthorized access, including illegal commercialization of data and data retention regulations covering data transferred beyond the original service supplier.

At a technical level, the grid and smart meter infrastructure appears as a network of networks, governed by partnerships and market-driven organizations, with an important input and regulation from the government. These partnerships manage, or will manage, large amounts of consumption and operational data, a fact which calls for a large effort in the direction of a "collaborative security" strategy with specified roles and a joint approach to prevent and repel cyber attacks.

Comprehensive security approach

A multi-faceted, defense-in-depth approach is required to ensure the overall security of the smart metering system. The security solution should aim to protect the system against known and unknown attacks (day zero attacks), unauthorized access, physical tampering, information compromise, denial of service, eavesdropping and other threats.

A set of preventive, detective and corrective controls should be implemented to ensure the security of the smart metering system, which includes end devices, management and monitoring systems, network infrastructure and payment environments. Some of the key controls necessary to meet the smart metering security requirements are: network segregation, data encryption (in transit and rest), near real-time monitoring, device/user authentication solution, device registration/deregistration, etc.

The control environment needs to be supported by a governance framework, appropriate policies and procedures, continuous monitoring and a maturity model to ensure that the overall smart metering system is protected against known and unknown issues and effectively responds to the changing threat landscape.

Customer data privacy and security are critical to ensure customer adoption of smart meters and the expected carbon footprint reduction. The principles of "privacy by design" and "security by design" are required for the implementation of security and privacy, and efforts in this area must be well understood, documented and visible to support the credibility of the solution.

It is important to highlight – as we did in the context of the connected car – that the entire issue of consumer and citizen data protection has not been resolved. There are large differences in legislation between countries and regions, and businesses face the lack of universally accepted technical or industrial standards.

A secure solution could only be achieved by taking a holistic view of the smart metering system and a structured approach to risk management. But to make it truly successful, security must be embedded into the initial solution and not viewed as an "add on."

For further perspectives around smart metering, please see EY's *Plug in* report (November 2014): www.ey.com/smartmeter

So how can organizations get ahead of cybercrime?

36%

of respondents do not have a threat intelligence program.**

37%

say that real time insight on cyber risk is not available.**

6%

of organizations claim to have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerability management function.**

Your organization may already have strong IT policies, processes and technologies, but, is it prepared for what is coming? Early warning and detection of breaches are decisive to being in a state of readiness, meaning that the emphasis of cybersecurity has changed to threat intelligence. Most organizations already know that there are threats for their information and operational systems, as well as for their products – the step beyond is to understand the nature of those threats and how these manifest themselves.

An organization in a state of readiness to deal with cyber attacks inhabits an entirely different mind-set, sees the world differently and responds in a way the cyber criminals would not expect. It requires behaviors that are thoughtful, considered and collaborative. It learns, prepares and rehearses. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience and limit damage from any given attack.

A state of readiness includes:

- Designing and implementing a cyber threat intelligence strategy to support strategic business decisions and leverage the value of security
- Defining and encompassing the organizations extended cybersecurity ecosystem, including partners, suppliers, services and business networks
- Taking a cyber economic approach – understanding your vital assets and their value, and investing specifically in their protection
- Using forensic data analytics and cyber threat intelligence to analyze and anticipate where the likely threats are coming from and when, increasing your readiness
- Ensuring that everyone in the organization understands the need for strong governance, user controls and accountability

Organizations may not be able to control when information security incidents occur, but they can control how they respond to them – expanding detection capabilities is a good place to start. A well-functioning security operations center (SOC) can form the heart of effective detection.

Managing cyber threats according to business priorities must be the focus of the SOC. By correlating business-relevant information against a secure baseline, the SOC can produce relevant reporting, enabling better decision-making, risk management and business continuity. An SOC can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively.

Follow leading cybersecurity practices

By leveraging-industry leading practices and adopting strategies that are flexible and scalable, organizations will be better equipped to deal with incoming (sometimes unforeseen) challenges to their security infrastructure.

As technology advances and companies continue to innovate over the coming years, organizations using the IoT will need to continuously assess the security implications of adopting these advancements. A consistent and agile multi-perspective security risk assessment methodology will help to evaluate the organizations risk exposure. The introduction of appropriate procedures and regular testing will help organizations become smarter and make their employees more aware of the challenges that IoT poses for the entire enterprise.

- Know your environment, inside and out
  Comprehensive, yet targeted, situational awareness is critical to understanding the wider threat landscape and how it relates to the organization. Cyber threat intelligence can bring this knowledge – it incorporates both external and internal sources of risk, and covers both the present and future, while learning from the past.
- Continually learn and evolve
  Nothing is static – not the criminals, not the organization or any part of its operating environment – therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics), maintain and explore new collaborative relationships, refresh the strategy regularly and evolve cybersecurity capabilities.
- Be confident in your incident response and crisis response mechanisms
  Organizations that are in a state of anticipation regularly rehearse their incident response capabilities. This includes war gaming and table top exercises, through to enacting complex incident scenarios that really test the organization's capabilities.
- Align cybersecurity to business objectives
  Cybersecurity should become a standing boardroom issue – a vitally important item on the agenda. The organization's leadership should understand and discuss how cybersecurity enables the business to innovate, open new channels to market and manage risk. To be successful, the information security function needs leadership support in providing the appropriate revenue to support and grow better security protection, to promote cybersecurity awareness within the workforce, and to sponsor cooperation with business peers.

Move from security as a cost, to security as a plus

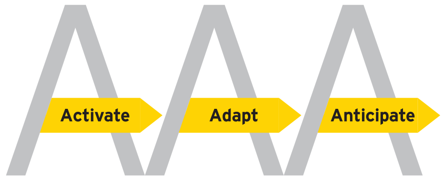
Security is usually positioned as an obligatory cost – a cost to pay to be compliant, or a cost to pay to reduce risk. But moving to a model of security as risk and trust management implies looking upon security as a business enabler; for example, managing consumer data access leverages the monetary value of the data instead of focusing on the protection of the data itself. In fact, this transformation means enabling the development of even more extended networks of networks, of more and new forms of collaboration and mobility, and of new business models. **"Security as a plus" should be a mainstay of the business.**

The future of IoT

"Dubbed by many as nothing less than the "3rd industrial revolution", the Internet of Things is one of the digital game changers. We believe that when everyone and everything is connected within seamless information networks and the resulting data is evaluated by intelligent and predictive big data analytics, and with robust cybersecurity measures in place, we will see positive changes in the way we all conduct business; how we operate our factories, supply chains and logistics networks; how we manage our infrastructure; and last but not least, how we as consumers, patients and citizens interact with suppliers, retailers, health care providers and government agencies."

Paul van Kessel, EY Global Risk leader

How can EY help?



EY has identified that organizations' responses to cybercrime fall into three distinct stages of cybersecurity maturity — Activate, Adapt and Anticipate (the three As) — and the aim should be to implement ever more advanced cybersecurity measures at each stage.

Stage 1: Activate

Organizations need to have a solid foundation of cybersecurity. This comprises a comprehensive set of information security measures, which will provide basic (but not good) defense against cyber attacks. At this stage, organizations establish their fundamentals – i.e., they "activate" their cybersecurity.

Stage 2: Adapt

Organizations change – whether for survival or for growth. Threats also change. Therefore, the foundation of information security measures must adapt to keep pace and match the changing business requirements and dynamics otherwise they will become less and less effective over time. At this stage, organizations work to keep their cybersecurity up-to-date; i.e., they "adapt" to changing requirements.

Stage 3: Anticipate

Organizations need to develop tactics to detect and detract potential cyber attacks. They must know exactly what they need to protect their most valuable assets, and rehearse appropriate responses to likely attack/incident scenarios: this requires a mature cyber threat intelligence capability, a robust risk assessment methodology, an experienced incident response mechanism and an informed organization. At this stage, organizations are more confident about their ability to handle more predictable threats and unexpected attacks; i.e., they anticipate cyber attacks.

What it is	Cybersecurity system building blocks	Status
Anticipate is about looking into the unknown. Based on cyber threat intelligence, potential hacks are identified; measures are taken before any damage is done.	Anticipate	**Anticipate** is an emerging level. More and more organizations are using cyber threat intelligence to get ahead of cybercrime. It is an innovative addition to the below.
Adapt is about change. The cybersecurity system is changing when the environment is changing. It is focused on protecting the business of tomorrow.	Adapt	**Adapt** is not broadly implemented yet. It is not common practice to assess the cybersecurity implications every time an organization makes changes in the business.
Activate sets the stage. It is a complex set of cybersecurity measures focused on protecting the business as it is today.	Activate	**Activate** is part of the cybersecurity system of every organization. Not all necessary measures are taken yet; there is still a lot to do.

Helping you anticipate cybercrime

We have seen that organizations need to change their way of thinking to stop being simply reactive to future threats; yet in our recent Global Information Security Survey (www.ey.com/cybersecurity) we found that only 5% of the 1,800 organizations surveyed had a threat intelligence team with dedicated staff.

The only way to get ahead of the cyber criminals is to learn how to anticipate their attacks; this means that your cybersecurity capability should be able to address the following questions:

- What is happening out there that our organization needs to learn from?
- How are other successful organizations dealing with threats and attacks?
- How can our organization become "hardened" against attack?
- Can our organization distinguish a random attack from a targeted one?
- What would be the economic cost of an attack?
- How would our customers be impacted by an attack?
- What would the legal and regulatory consequences of a serious attack be?
- How can we help others in our ecosystem deal with threats and attacks?

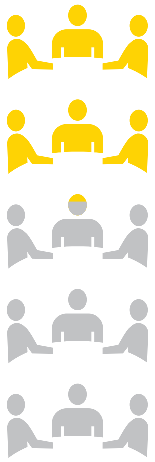
EY can help organizations improve their ability to respond to changes in the threat landscape. We provide services to assist organizations in developing in-house threat intelligence programs as well as several key threat intelligence services in subscription-based models and full spectrum managed cyber threat intelligence services.

We believe that security assessments are an effective method of identifying vulnerabilities and understanding their impact. Together with IT security, risk management and internal audit groups at our clients, we contextualize these technical findings within the business to fully understand the risk to the most critical assets. It is this teaming between technical testers and business owners that we believe will continue to be the most effective method of evaluating the security of both established and emerging technologies.

Using EY's security practices and industry leading experience, we help our clients secure both the device ecosystem and assess security at the network level, and we assist our clients in defining and implementing state-of-the-art security controls to:

- Secure the data from device to data center to the cloud
- Manage large volumes of data, utilizing our knowledge of data analytics
- Comply with the applicable security and regulatory requirements
- Standardize the security controls for their offerings, thereby creating faster go-to-market capabilities

However, we appreciate that many of our clients face location, time and cost constraints, which make it difficult to determine what security measures are cost-effective and make sense within the business strategy. We can help our clients gain a thorough understanding of the options.



58%

of organizations do not have a role or department focused on emerging technologies and their impact on information security.**

IoT must change the way businesses do business

There is no doubt that IoT is changing the way we all live and work. There are many opportunities for the public as well as private sector markets through technological integration and collaboration.

New innovations are being introduced daily, but along with these, threats are being created which will challenge your organization. You need to get ahead of the game now to be successful tomorrow.

IoT will increasingly have sensing, analytics and visualization tools that may be accessed on a personal, community or national level. Information sharing and ease of accessibility via the IoT makes businesses vulnerable to targeted cyber attacks, so the huge benefits must be weighed against the growing risks.

> IoT offers tremendous opportunities for personal improvements and for business innovation, but innovators need to be aware of the risks involved in IoT to provide better and more powerful solutions for the world.
>
> *Ken Allan, Global Cybersecurity Leader, EY.*

As a consequence of IoT adoption, together with supporting technologies and services based on cloud infrastructure and mobile devices, enterprise security requirements have to be addressed with a focus on the relationships between the organization and its environment.

Organizations must adapt and look ahead and beyond the current business. With the understanding that attacks can never be fully prevented, companies should advance their cyber threat detection capabilities so they can respond appropriately and proactively.

Learning how to stay ahead of cybercrime is challenging and takes time, but the benefits for the organization are considerable – the organization will be able to exploit the opportunities offered by the digital world, while minimizing exposure to risks and the cost of dealing with them.

Next steps

Take a look at your organization (public, private or NGO). What can you do that you couldn't do before? Start to do it now, before someone else does. "Act" rather than "react."

Consider these key questions:

- What IoT capabilities does your organization have today?
- Can you harness the complementary insights of both service and IT leaders?
- Have you identified major IoT opportunity areas that link with your vision and strategy?
- Can you build an "IoT culture" around the possibilities of connecting the unconnected?
- How will IoT change the basis of competition?
- How will you delight customers as everything gets connected?
- Do your business plans reflect the full potential of IoT?
- Are your technology investments aligned with opportunities and threats?
- How will IoT improve your agility?
- Do you have the capabilities to deliver value from IoT?
- What is your accountability and governance structure/ model for IoT execution?
- How are the risks associated with IoT being addressed?
- How will you communicate about IoT to stakeholders?

If you are unsure about any of these answers, speak to your EY representative.

Want to learn more?

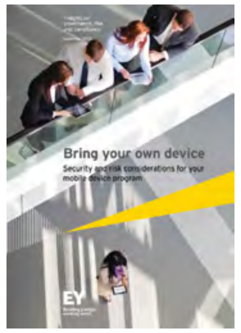
Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our *Insights on governance, risk and compliance* series at www.ey.com/GRCinsights.

Get ahead of cybercrime: *EY's Global Information Security Survey 2014*

www.ey.com/GISS

Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem


Bring your own device
Security and risk considerations for your mobile device program
EY

Bring your own device: *security and risk considerations for your mobile device program*

www.ey.com/byod

Security Operations Centers – helping you get ahead of cybercrime
EY

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Cyber Program Management: *identifying ways to get ahead of cybercrime*

www.ey.com/CPM

Cyber threat intelligence – how to get ahead of cybercrime

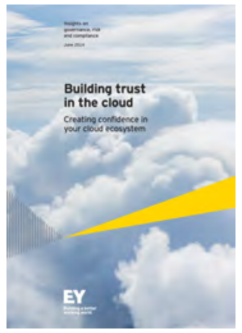
www.ey.com/CTI

Maximizing the value of a data protection program

www.ey.com/dataprotect

Big data: *changing the way businesses compete and operate*

www.ey.com/bigdatachange


Building trust in the cloud
Creating confidence in your cloud ecosystem
EY

Building trust in the cloud: *creating confidence in your cloud ecosystem*

www.ey.com/cloudtrust

At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

We innovate in areas, such as risk consulting, risk analytics and risk technologies, to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our client's applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. AU2979
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com/GRCinsights

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or, more specifically, on achieving growth or optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory

Our Risk Advisory leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp