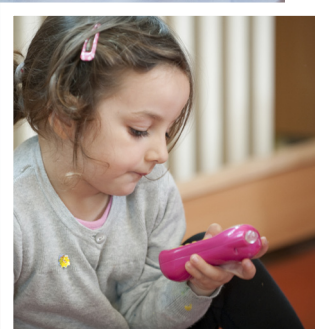
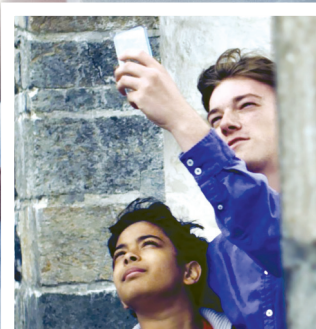
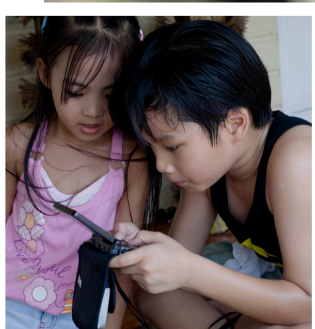


# Building Digital Resilience



## Table of Contents

Executive summary	3
Section 1: Growing access to mobile internet services	4
Section 2: Risk posed to children by mobile internet services	6
Section 3: Risk and resilience varies across the world	7
Section 4: Building resilience and reducing risk to minimize harm	8
Section 5: Stakeholders have diverse roles to play	10
Section 6: Telecoms companies are already playing an important role	12
Section 7: Telecoms companies can still do much to reduce the risks	13
Appendix: Building Digital Resilience – Country analysis	14
Sweden	14
Malaysia	17
Montenegro	20
Building Digital Resilience – Bibliography	
Key books and articles	23
Primary websites and other resources	24

## Executive summary

The spread of mobile internet services around the globe has occurred at a rapid pace. This expansion has changed lives for millions of people, with mobile devices providing unprecedented voice, video and social media communication capabilities and instant access to a vast range of information and entertainment services. In the process, mobile internet access is also quickly becoming part of life for children and young people. This brings with it substantial benefits, but also risks. What this means is that if the gains of mobile internet for children are to be reaped while mitigating the risks, companies, governments and other stakeholders need to work closely together.

Children are the world's "digital natives"—growing up not only taking for granted the presence of technology in their lives, but also ownership of a mobile device. In short, mobile internet is increasingly becoming part of daily life for children.

In general, the increase in children's access to online services is overwhelmingly positive, bringing with it educational and developmental benefits as well as security, giving parents the ability to keep track of their children wherever they are and to communicate easily with them when plans change or they are running late. Expansion of internet access to this cohort also generates long-term socio-economic benefits, increasing digital literacy and building skills they will need to succeed in the 21<sup>st</sup> century.

However, along with the opportunities, some serious risks also come with the technology. Children can be passive victims of harm—whether that is being exposed to unwanted information, disturbing images or contact from online sexual predators. But they can also be active participants, engaging in cyber-bullying of their schoolmates or distributing inappropriate content about their peers via their social media networks.

The risks do not necessarily always translate in to harm. Skills training, teacher and parent support, and awareness raising all help build resilience in children. This can be supplemented with filtering or blocking technology and the creation of appealing positive content. Legislative frameworks can also be used to encourage industry participation and reduce the amount of potentially harmful content available online.

Yet the degree of resilience, the exposure to the risks, and how these develop will vary considerably between countries, depending on factors such as the use of mobile devices by children in that country and the level of IT awareness among both parents and children. It is critical that attempts to protect children should not come at the expense of children's privacy rights and the ability for young people to benefit from the rich seams of education and entertainment available on the web.

What is clear, however, is that potential risks will continue to increase as the uptake by children and young people of mobile internet services rises. For government and citizens in all countries, measures will need to be taken to reduce risks and increase resilience. Thoughtful legislation is a necessary step. However, given the complex range of issues presented by childhood use of mobile internet, regulation alone cannot deliver mobile services for children that pose fewer risks and minimize the potential for harm.

What this means is that a diverse group of stakeholders—from government agencies to private sector companies, schools, civil society groups and individual citizens, will need to collaborate. Ultimately, parents are the most critical stakeholders, facing the challenge of balancing use of tools that minimize risk with the need to respect their child's right to privacy and his or her ability to benefit from online access. However, without co-operation from all stakeholders, maximizing the benefits of mobile internet for children while minimizing the risks cannot be achieved. And in this endeavour, of course, a key role exists for the providers of these services—the telecommunications companies.

## Section 1: Growing access to mobile internet services

*“In 12 study markets, it is anticipated that the number of children online will reach some 176 million by 2017”*



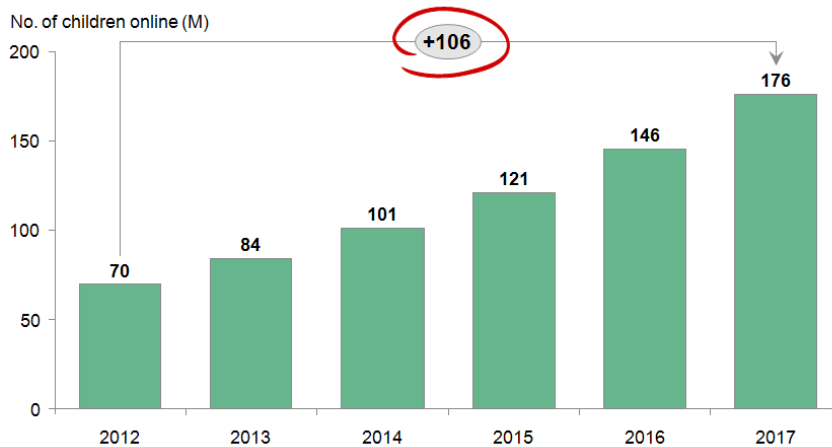
With global market penetration approaching 100%, mobile technology is reaching the hands of everyone across the world. The increase in penetration has been rapid. In just over a decade between 2000 and 2011, mobile subscriptions increased from less than a billion to some 6 billion worldwide. In the same period, internet users rose in number from half a billion to 2.3 billion—an increase of an astonishing 453%.

For countries, this is good news. Mobile access helps generate economic growth. Studies have shown that with just a 10% rise in internet penetration, new business creation increases by 1%, as does gross domestic product. There are gains for society, too, with increased government transparency and freedom of expression, improved education levels, incomes and lifestyles and greater access to financial services and healthcare.

And a growing number of mobile internet users are children and young people. In 12 study markets, it is anticipated that the number of children online will reach some 176 million by 2017, an increase of 106 million from 2012, with approximately 85 million of these children using a mobile device when going online for the first time.

### ~100 million new children will come online by 2017

Expected to reach 176 million online children in 2017 in 12 study markets



**~85 million of these children will use a mobile device when going online for their first time**

Note: Based on individuals between ages of 5-17  
Source: World Bank Data; BMI; EIU; United States Census Bureau; BCG analysis

THE BOSTON CONSULTING GROUP

*~100 million new children will come online in study countries by 2017*

For children and young people, access to mobile internet services creates a wide range of educational, economic and lifestyle opportunities. For a start, children have fun online and on their mobiles. These devices provide ways for them to communicate with friends, engage with each other through social media, and gain access to instant entertainment.

While they are engaged in these activities, children are also learning and acquiring skills that will enhance their lifestyles, whether they are building their ability to research travel destinations and access essential services or they are developing their powers of creativity and self-expression. As Unesco, the United Nations' cultural agency, has stressed, digital literacy is as relevant as reading and writing, mathematics or the management of social behaviour.

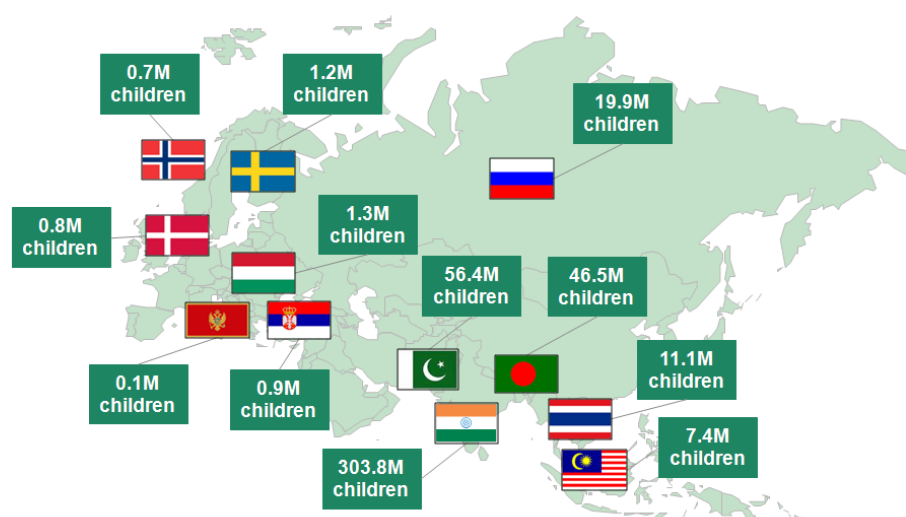
Some of the skills children and young people acquire online on mobile devices relate directly to their future economic prospects—whether enhancing their employability or building entrepreneurial skills. This is particularly important given the growing requirement for IT literacy on the part of most employers, including those hiring people for what were traditionally known as “blue collar jobs.” In the workplace, research, data, lectures, training, debates and collaboration between teams are all moving online, which means tomorrow's employees will be expected to have extensive experience in using online tools.

As they start to build lives for themselves, young people will also need to know how to access public services (which are also increasingly moving online) and how to manage the healthcare of themselves and their families through new digital mHealth services. And, of course, online social networks and different forms of entertainment delivered via the web are becoming an increasingly important part of leisure time.

With the advantages of online mobile services spreading beyond direct users, by 2017 approximately 450 million children in the 12 study markets could benefit from internet use, whether or not they are direct subscribers.

## ~450M children in 12 study markets could benefit from the Internet, even if they are not users directly

Projected total number of children (age 5-17) in 2017 in study markets



Note: Number of children based on individuals between ages of 5-17  
Source: World bank data, US Census Bureau, BCG analysis

THE BOSTON CONSULTING GROUP

~450M children in 12 study markets could benefit from the Internet

## Section 2: Risk posed to children by mobile internet services

*“Children can either be passive victims or themselves perpetrators of risky or undesirable behavior”*



While increased mobile internet use means more children are taking advantage of the opportunities they find online, inextricably linked to this are a number of online risks. Worries range from the ability of advertisers to target young people with ads for inappropriate products to the fact that the web can facilitate cyber-bullying and enable sexual predators, who can disguise their identity to contact their targets more easily. While it is possible to take steps (especially at the end-user level) to reduce risk exposure, it is also critical to focus on building the resilience that can minimize harm from online encounters with malicious individuals or inappropriate content.

The risks are varied in nature. For example, incidents such as children spending thousands of dollars on in-app purchases, suicides of teenagers as a result of online bullying and youth riots instigated by online harassment have appeared in the news media. In some cases, concern about this has translated into action with initiatives that include proposing new legislation that clearly outlaws online hate speech and harassment.

Meanwhile, the technology can enable young people themselves to engage in undesirable behavior, including cheating on school tests and using the internet to bully their schoolmates.

As the examples above indicate, children can either be passive victims or themselves perpetrators of risky or undesirable behavior, or even crimes. The resulting harm can take various forms—social, financial, legal, physical or psychological—and can be inflicted via a number of channels—through content, contact, commercial transactions or security breaches.







For the victims, this can mean exposure to undesirable or dangerous content that is pornographic, violent or racist or promotes harmful behavior through online content such as websites encouraging anorexia or suicide. Victims may also suffer through contact with cyber-bullies, cyber-stalkers or those who groom children online, befriending them in preparation for sexual activity.

When it comes to commercial risks, these include approaches from marketers promoting age-inappropriate or illegal products to youngsters or persuading them to enter into purchase agreements unknowingly. Meanwhile, numerous security risks face children online from unknowingly installing malicious programs on their devices to falling victim to fraud, phishing (false acquisition of data such as usernames, passwords and credit card details) or identity theft.

Young people can also be active perpetrators of undesirable behavior, misdemeanors or crimes online. Some generate and distribute through their networks potentially harmful content such as explicit images or racist content, hate speech or politically extreme blog posts.

Others may engage in activities such as “sexting” their peers or younger children (sending them sexually explicit messages or photographs via their mobile devices) or harassing or cyber-bullying them. Some infringe copyrights by, for example, downloading films or music. Others gamble or go on excessive online spending sprees. Technologically savvy young people can also breach security barriers by disclosing the personal information of others on social networking sites or by hacking into the computers of companies or individuals.

## Children face a wide range of risks online

Child's role Type of risk	 Passive	 Active
 Content	<ul style="list-style-type: none"> <li>Viewing pornographic / violent / racist content</li> <li>Viewing other potentially harmful online content (e.g., pro-anorexia, pro-suicide)</li> </ul>	<ul style="list-style-type: none"> <li>Generating / posting potentially harmful content (e.g., explicit pictures, blog posts)</li> </ul>
 Contact	<ul style="list-style-type: none"> <li>Being cybergroomed<sup>1</sup></li> <li>Being harassed / stalked</li> <li>Being cyber bullied</li> </ul>	<ul style="list-style-type: none"> <li>"Sexting"</li> <li>Harassing others</li> <li>Cyber bullying others</li> </ul>
 Commerce	<ul style="list-style-type: none"> <li>Marketing of age-inappropriate / illegal products</li> <li>Unknowingly entering into purchase agreements</li> </ul>	<ul style="list-style-type: none"> <li>Infringing on copyrights</li> <li>Gambling (excessively) online</li> <li>Purchasing (excessively) online</li> </ul>
 Security	<ul style="list-style-type: none"> <li>Unknowingly installing malicious code (e.g., viruses and spyware)</li> <li>Being the victim of fraud / phishing</li> <li>Being the victim of identity theft</li> </ul>	<ul style="list-style-type: none"> <li>Disclosing personal information (e.g., on SNS<sup>2</sup>)</li> <li>Hacking</li> </ul>

<sup>1</sup> Actions undertaken with the aim of befriending and establishing an emotional connection with a child to lower the child's inhibitions in preparation for sexual activity <sup>2</sup> Social Networking Sites  
 Note: Illustrative examples of risks within each Category – not meant to be exhaustive  
 Source: EU Kids Online, OECD, ITU, YPRT, BCG analysis

THE BOSTON CONSULTING GROUP

### Children face a wide range of risks online

Worryingly, many are already encountering risks. Evidence from a range of studies on online risks suggest that among the 67 million online children in the 12 study markets, ~14 million could have been exposed to potentially harmful user-generated content and up to 35 million may have experienced cyber-bullying, while about 17 million might have talked online to someone they did not know. Security breaches were also common in the studies, with up to 6 million children having been potentially subject to some type of personal data misuse.

## Section 3: Risk and resilience varies across the world

While children and young people share many of the same hopes and fears—and are therefore equally vulnerable to the risk of harm from online mobile content, the risks they face and their resilience to either avoid risks or recover from harm vary across the world due to a range of factors, including differences in amount and characteristics of usage.

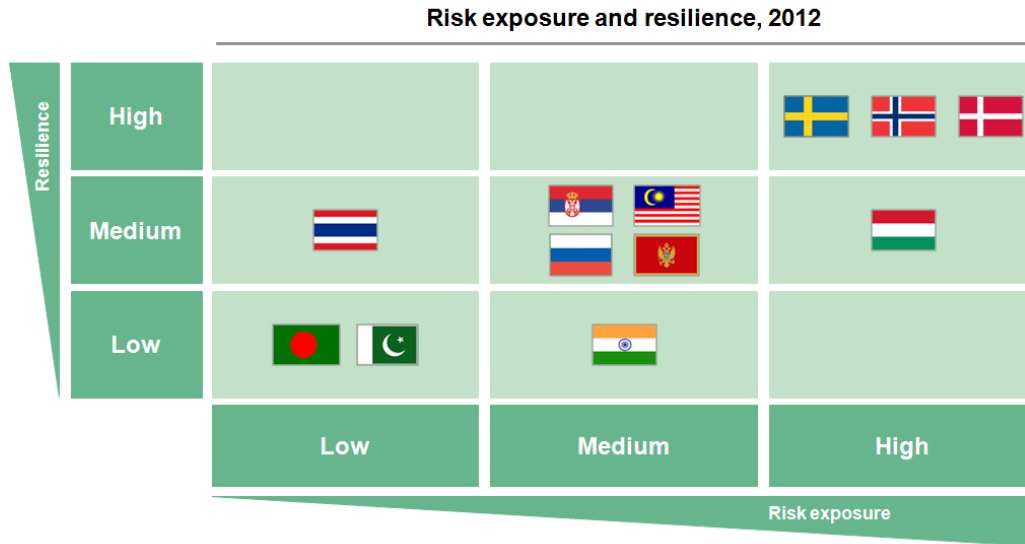
First, it is the case that the more a child uses the internet, the more he or she is likely to encounter potentially harmful sites or individuals online. Moreover, children using personal or mobile devices are at greater risk since these personal devices are less easy to control than a home or school-based computer shared by others. Their ability to access potentially harmful content will also vary from country to country.

Based on 2012 data on these factors, some countries emerge as places where children are at higher risk than others. Denmark, Norway, Sweden and Hungary are high-risk countries. Malaysia, India, Russia, Montenegro and Serbia are at medium risk while in the low risk group are Bangladesh, Thailand and Pakistan.

Similarly, the ability to withstand harm from risks varies from country to country. Here, education plays an important role with higher educational levels and ICT and internet skills correlating with higher levels of resilience. Children with more online experience will also be better able to handle risks when they encounter them. And countries that possess strong institutions can help protect their citizens from online risks and move quickly to meet new risks and changing environments.

In this respect Sweden, Norway and Denmark have high levels of resilience while Malaysia, Serbia, Hungary, Russia, Thailand and Montenegro have medium levels of resilience with the lowest levels found in Bangladesh, India and Pakistan.

## Harm from risk exposure partially mitigated by resilience



Source: EIU; ITU; WEF; BMI; World Bank; Communication Chambers; IMF; OpenNet Initiative; Reporters Without Borders; IC Intelligence Center; BCG analysis  
THE BOSTON CONSULTING GROUP

### Harm from risk exposure partially mitigated by resilience

While some countries are clearly better equipped to manage online risks relating to children, even these countries cannot afford to relax their focus on this issue but should create policies that increase their resilience and further minimize the risks.

## Section 4: Building resilience and reducing risk to minimize harm

*“Building resilience among young people will ultimately be the more powerful strategy”*




While the dangers children can be exposed to through mobile internet are very real, much can be done to reduce the likelihood of young people encountering potentially harmful content or individuals online.

Risk-mitigation measures can help lower the likelihood of children being exposed to harmful content. These include using clean content labeling that makes it easy for children and parents to identify age- and child-appropriate material while also creating more high-quality content that will be appealing to children and young people.

A basic pre-requisite for risk reduction is legislation. Clearly defining and outlawing certain online content, such as child abuse materials, reduce the risk of young people being exposed to this material, as does active prosecution of the perpetrators of crimes such as cyber-grooming. However, tough legal measures will never be sufficient – other levers are required to maximize the benefits of online access while simultaneously seeking to minimize harm.



Monitoring and moderating of online activities is one such lever. This means providing parents with the means to keep an eye on their child’s use of online content. It could also include moderating of social media and chat rooms where children interact with each other, but where they are at risk of unwanted or harmful contact.

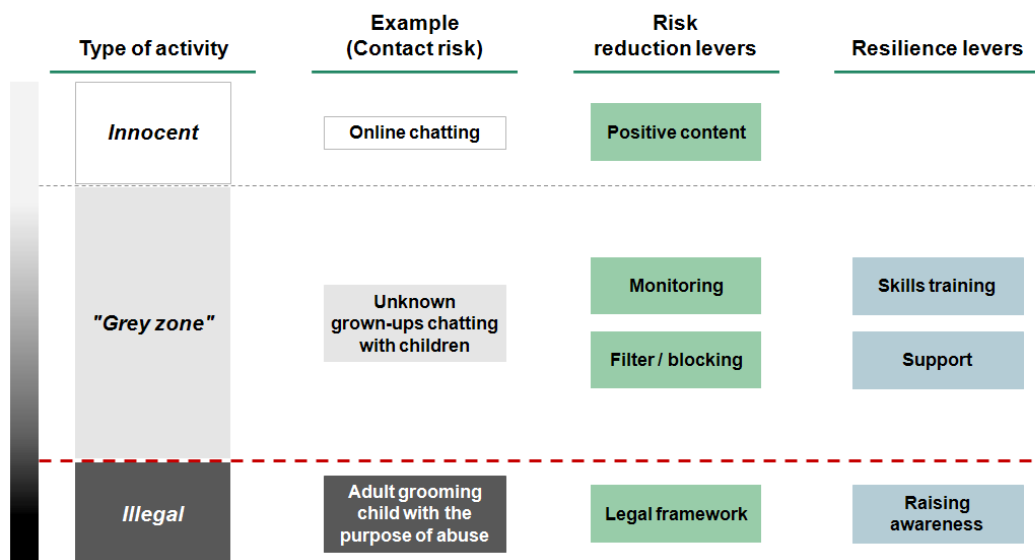
Technology plays a role, too. As well as antivirus software, parents or teachers can install software programs that will filter out certain sites from web searches and blocks specific applications, websites or content. These programs can also be used to verify the age of users of mobile internet sites and control the amount of time a child spends online. However, users should remember to strike the right balance between harm prevention and a child’s right to privacy.

While it might be tempting to focus narrowly on risk reduction through technology or legislation, building resilience among young people – what might be termed “filters in the mind” - will ultimately be the more powerful strategy. This requires helping them either learn how to avoid harmful online encounters or seek help when they do, and thereby recover more quickly after coming across dangerous or inappropriate web content.

Resilience building takes a number of forms. First, raising awareness of the risks among young people and their parents is important. This could be done through an online school promoting safer internet use or the distribution of awareness information targeting both parents and their children. The next step is building skills that can help reduce risk of harm. At school, internet safety can be taught as a subject while smartphone or web-based applications and other ICT products help parents and children manage the risks.

To effectively build resilience and mitigate risk, support is needed from a wide variety of stakeholders, along with industry collaboration and self-regulation. As with so many of the dangers facing society today, no one actor can reduce the risks. Mobile online content cuts across parental, educational, technological, governmental and corporate responsibility. Therefore all members of society must bring to bear their capabilities and strengths in reducing the potential for harm.

## Legal framework will never be sufficient – other levers needed to reduce risk and increase resilience

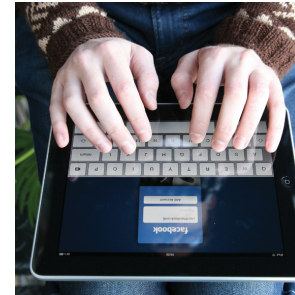


THE BOSTON CONSULTING GROUP

*Legal framework will never be sufficient*

## Section 5: Stakeholders have diverse roles to play

*“Parents need to balance risk mitigation with their children’s right to privacy and potential to learn and grow through their use of online content”.*



### Diverse stakeholders must collaborate to succeed ...

Example: Comprehensive solution to cyber bullying requires multi-stakeholder involvement

Mitigating action	Activities to tackle cyber bullying (exemplars)	Key stakeholder(s)
Skills training	<ul style="list-style-type: none"> <li>Teaching children how to block messages from specific senders</li> <li>Teaching children critical thinking – increasing understanding of potential consequences of cyber bullying</li> </ul>	<ul style="list-style-type: none"> <li>Educators</li> <li>Parents</li> </ul>
Support	<ul style="list-style-type: none"> <li>Helplines / online communities where children can seek guidance</li> <li>Easily approachable adults for discussing cyber bullying</li> <li>Reporting tools (site-specific and / or general)</li> </ul>	<ul style="list-style-type: none"> <li>Parents</li> <li>Civil society</li> <li>Content/service providers</li> </ul>
Raising awareness	<ul style="list-style-type: none"> <li>Cyber bullying awareness programs targeted at parents, children, teachers</li> <li>Discussing cyber bullying in school and at home with parents</li> </ul>	<ul style="list-style-type: none"> <li>Educators / civil society</li> <li>Connectivity providers</li> <li>Parents</li> </ul>
Positive content	<ul style="list-style-type: none"> <li>Offering educational / entertainment content addressing / discussing issue of cyber bullying</li> </ul>	<ul style="list-style-type: none"> <li>Content/service providers</li> <li>Civil society</li> <li>Parents</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>Moderating of chat rooms, discussion forums, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Parents</li> <li>Content/service providers</li> </ul>
Filter / blocking	<ul style="list-style-type: none"> <li>Technical tools to block messages from specific sender(s)</li> <li>Option to block access to personal online profiles for specific individuals</li> </ul>	<ul style="list-style-type: none"> <li>Parents</li> <li>Content/service providers</li> <li>Connectivity providers</li> </ul>
Legal framework	<ul style="list-style-type: none"> <li>Clear legal framework outlining illegal online harassment, statements, etc</li> </ul>	<ul style="list-style-type: none"> <li>Authorities</li> </ul>

THE BOSTON CONSULTING GROUP

### Diverse stakeholders must collaborate to succeed

Ultimately, responsibility for children’s safety online will lie with their parents. It is they who need to bring up the subject of online risks and to encourage their children to discuss their online life with them. However, it will also take action from all sectors of society to balance the benefits of mobile internet for children and young people while protecting them from harm. And in these efforts, since different stakeholders bring different strengths to the table, each should focus on harnessing their unique advantages.

Participation is certainly required by the children themselves. As first-hand users with direct experience of online risks and harm, children have unique insights to bring to the table, while at the same time having great potential to act as mentors towards their peers. It is therefore critical to allow their voices to be heard.

Further, active involvement from parents and other family members is needed. With intimate knowledge of their children’s online habits and desires, parents are most likely to be the first to notice when something is wrong. And family members can encourage mentoring between siblings or between older relatives and the children in the family.

Parents need to balance risk mitigation—through use of different tools and technologies—with their children’s right to privacy and potential to learn and grow through their use of online content. Moreover, risk exposure also builds their resilience, so shielding a child completely might make handling online risks more difficult when they become adults.

Parents should also work closely with their children’s educators. This means not only equipping children with technical skills, such as how to block messages from certain senders, but also teaching them to think more broadly about the potential consequences of online activities such as cyber-bullying. Similarly, educators and parents together play a role in delivering awareness raising programs.

With a prominent place in children’s daily lives, educators are in a unique position to reach out to children and parents and to keep track of children’s activities online. They can also draw upon their expertise in teaching to disseminate information and advice and are able to harness the potential of peer-based monitoring and support.

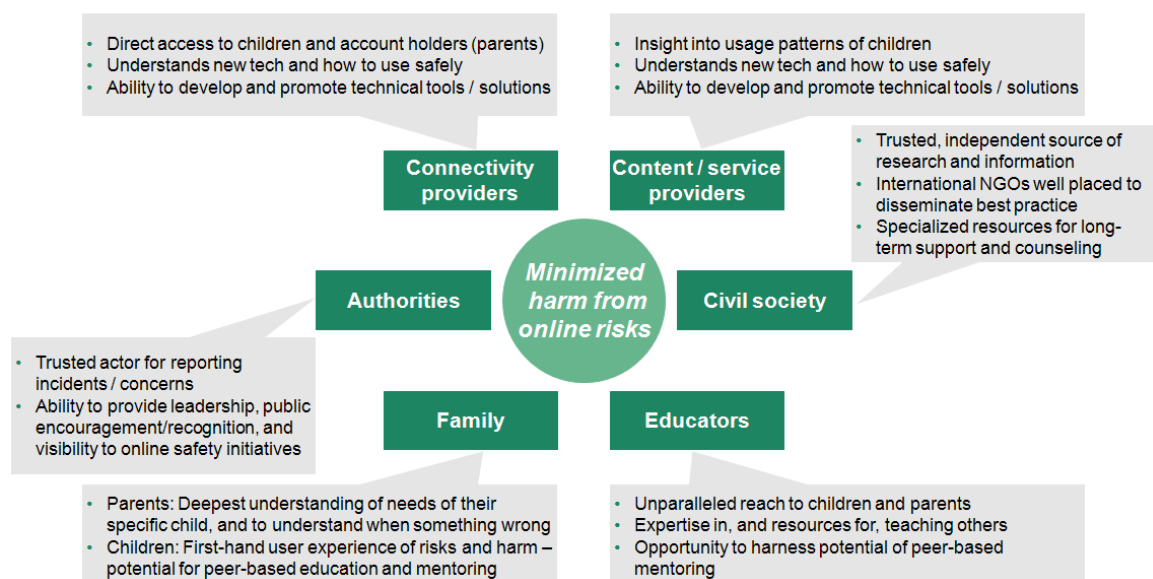
When it comes to support services, parents, civil society groups and content or service providers need to collaborate to provide helplines and online communities to which children can turn for assistance and guidance. Provision of online reporting tools can also give children and young people mechanisms through which to note any inappropriate content or contact they encounter on the web.

In addition to training, awareness raising and support services, much can be done by content and service providers to tailor the online experience for children in such a way as to reduce their risk of encountering potentially harmful content or contact. This includes providing positive content—such as safe chat rooms and age-appropriate entertainment—as well as developing technical solutions that can block and filter unwanted content and prevent access to certain online groups and individuals.

Government plays a role here, too. As well as providing leadership and visibility for these issues, government agencies are trusted institutions and therefore are able to help when it comes to the reporting of incidents and concerns. They can also support online safety initiatives both by publicly encouraging and recognizing them but also setting aside resources—whether financial or human—to accelerate their development. Governments must also establish legal frameworks that are technologically neutral but clearly delineating the boundary of criminal acts, whether they are conducted online or offline. Governments can also provide the resources and develop the capabilities needed to prosecute offenders.

With a similarly respected standing in society, international non-governmental organizations (NGOs) are well placed to provide research resources on issues of mobile internet security for children. They can disseminate best practice, provide specialized resources for long-term support and counseling and build relationships with children, parents and educators.

## ... each bringing unique advantages that should be leveraged



Source: eNACSO; ITU; EU Kids Online; OECD; BCG analysis

THE BOSTON CONSULTING GROUP

*Each stakeholder brings unique advantages that should be leveraged*

## Section 6: Telecoms companies are already playing an important role

The good news is that, when it comes to reducing the risk to children from online activity, much is already being done, and telecoms companies are playing an important role in working to reduce the prevalence of content that is harmful to children and developing technical filters that block access to child abuse materials.

First, they are taking measures to reduce the availability of online materials that could be used to abuse children. For example, one telecoms industry initiative—with companies working closely with relevant authorities in each market—has introduced measures to stop the spread of online child abuse materials.

Another service being offered by telecoms companies to all their customers is a technical filter addressing cyber-bullying by blocking messages from specific senders. These messages are available to parents so that they can be made aware of the problem. Meanwhile, senders are notified of the fact that they are being blocked and why.

Educational programs are another way telecoms companies are addressing online risks for children. In several countries, a “safe internet ambassador” program has been introduced. Children enrolled in the program are trained in advanced internet skills before being named “ambassador” and returning to support their peers, teachers and parents.

In addition, as part of school outreach programs designed to raise awareness around cyber-bullying, representatives from telecoms companies are traveling to schools to encourage debate and reflection among schoolchildren, parents and teachers about cyber-bullying. The program—a collaboration between the telecoms sector, NGOs and local authorities—has yielded strong evidence that its participants acquire the skills needed to avoid cyber-bullying.

Despite these efforts, however, more activities need to be rolled out in both developed and developing markets—and involving all stakeholders—if the benefits of mobile internet services are to be increased while reducing the risk of harm.

### Call to action: Roll out activities to reduce harm in all markets

Study experiences and best practices in other markets	Generate independent, research based evidence	Remain vigilant towards current and emerging risks
 Family	 Family	 Family
 Educators	 Educators	 Educators
 Civil society	 Civil society	 Civil society
 Connectivity providers	 Connectivity providers	 Connectivity providers
 Service/content providers	 Service/content providers	 Service/content providers
 Authorities	 Authorities	 Authorities

**~100 million new children online in study markets by 2017 – now is the time to build digital resilience!**

THE BOSTON CONSULTING GROUP

*Call to action: Roll out activities to reduce harm in all markets*

## Section 7: Telecoms companies can still do much to reduce the risks

*“As providers of online access telecoms companies can and should play a leading role in providing solutions”.*



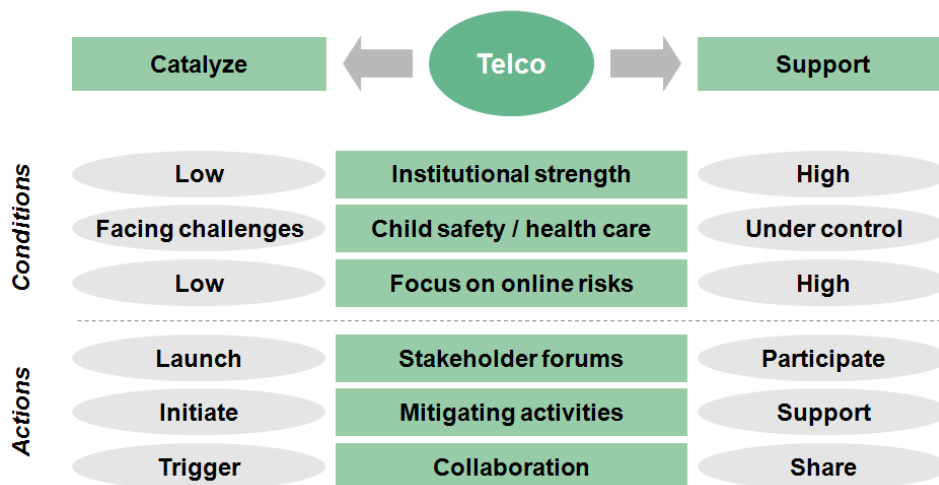
Central to mobile internet use are telecoms companies—the content, service and connectivity providers. Through their relationship with existing customers, these companies have direct access to those potentially at risk through delivery of service. They also have a deep understanding of the technology, how children and young people use it, how it is evolving and how it can be used safely. As such they are able to develop and market improved technical solutions to mobile internet risk. Through their relationship with customers and their technical and operational know-how, telecoms companies also have the ability to develop and disseminate information and technical tools directly to users—as well as to other stakeholders.

As multinational organizations working across borders, telecoms companies can take lessons learned from one market and apply it to another. Moreover, these companies have acquired extensive experience in adapting to rapidly changing markets. As providers of online access telecoms companies can and should play a leading role in providing solutions. Of course, depending on the nature of individual markets, telecoms companies will either support existing institutions and initiatives, or catalyze action.

Where strong government institutions and legal systems are in place, child health and safety systems are well developed and stakeholders have a strong focus on the risks posed to by children accessing online services, telecoms companies can play a supporting role. This means supporting, where relevant, activities designed to reduce the risk of harm. It also entails collaboration with government agencies and civil society groups, as well as participating in stakeholder forums to share their technical competence and deep knowledge of their markets and customers.

By contrast, in places where institutional and stakeholder attention to the welfare of children online is lacking and health and safety mechanisms for youngsters are weak, telecoms companies may need to catalyze action. In such places, they might initiate partnerships with authorities and civil society groups or launch stakeholder forums to address online risks and implement solutions. They may also take on greater responsibility for initiating and coordinating awareness-raising campaigns.

### Nature of role varies with market characteristics



Source: Expert interviews; BCG analysis

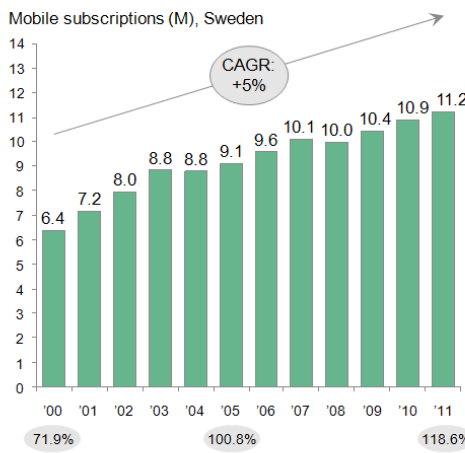
## Appendix: Building Digital Resilience – Country analysis

### Sweden

In the past decade, Sweden has seen a compound annual growth rate of 5% in mobile subscriptions, with penetration rates rising from just under 72% to almost 119%. In the same period, the number of internet users has more than doubled, rising from 4 million to 8.6 million, with penetration rates increasing from approximately 46% to almost 91%. By 2017, the number of children online in Sweden is expected to reach 1.2 million, a compound annual growth rate of 1%, with penetration rising from almost 92% to more than 98%. The country faces a high risk exposure but also has a high level of resilience.

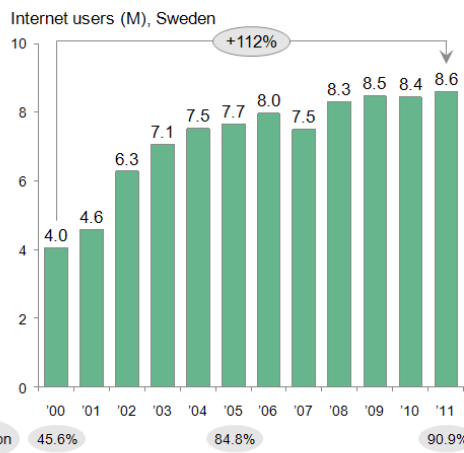
### Sweden has seen significant increase in access to mobile and online services last decade

**Mobile technology placed in "everyone's" hands**



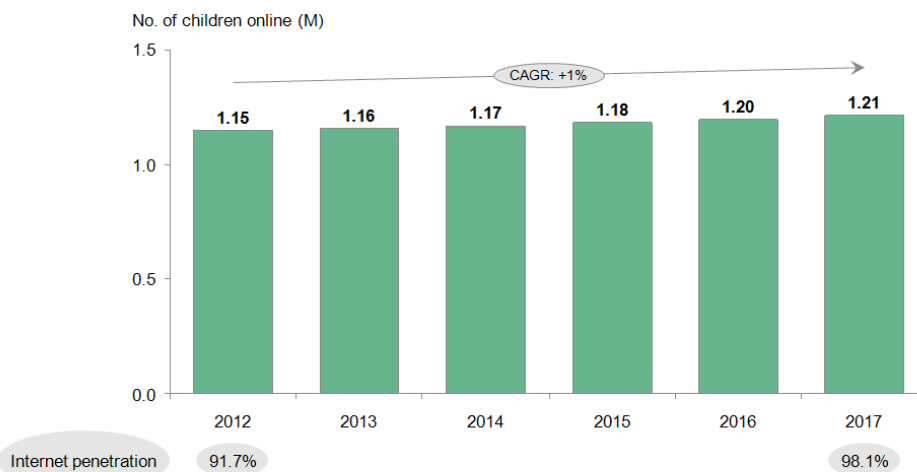
Source: World Bank; BCG analysis

**Number of internet users more than doubled**



THE BOSTON CONSULTING GROUP

### ~1.2 million children in Sweden expected to be online by 2017

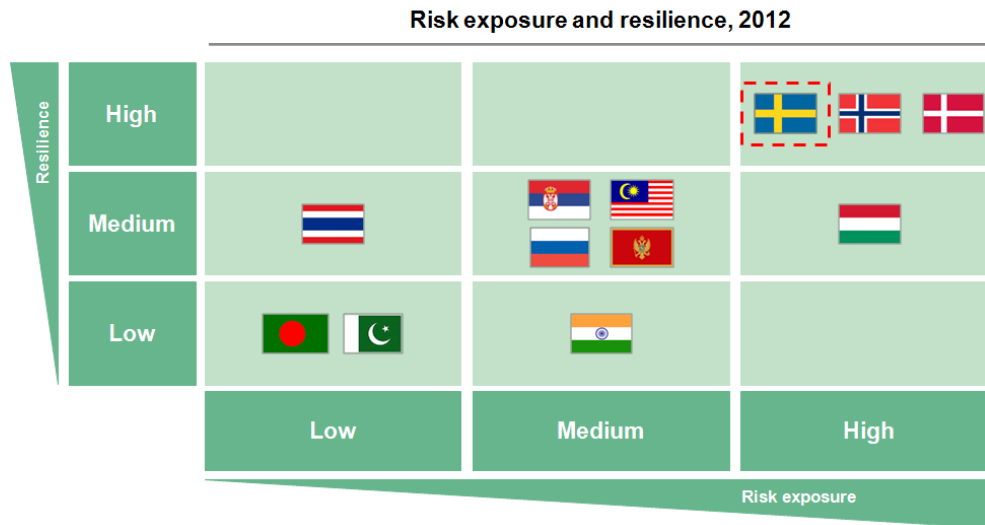


Note: Based on individuals between ages of 5-17  
Source: World Bank Data; BMI; EIU; United States Census Bureau; BCG analysis

THE BOSTON CONSULTING GROUP

## Harm from risk exposure partially mitigated by resilience





Sweden faces high risk exposure, but also has high resilience



Source: EIU; ITU; WEF; BMI; World Bank; Communication Chambers; IMF; OpenNet Initiative; Reporters Without Borders; IC Intelligence Center; BCG analysis  
 THE BOSTON CONSULTING GROUP

## Diverse stakeholders must collaborate to succeed

Example stakeholder organizations in Sweden

<p style="text-align: center;"><b>Connectivity providers</b></p>  <p style="text-align: center;"><b>Authorities</b></p>  <p style="text-align: center;"><b>Family</b></p> <ul style="list-style-type: none"> <li>• Children</li> <li>• Parents &amp; other caregivers</li> </ul> <p style="background-color: #f0f0f0; padding: 5px;"><b>Ultimate responsibility lies with parents, but other stakeholders need to provide support</b></p>	<p style="text-align: center;"><b>Content and service providers</b></p>  <p style="text-align: center;"><b>Civil society</b></p>  <p style="text-align: center;"><b>Educators</b></p> <ul style="list-style-type: none"> <li>• Schools</li> <li>• Youth clubs etc.</li> <li>• Community organizations</li> </ul>
---	--

Note: Logo's illustrative of organizations within each stakeholder group – not meant to be exhaustive  
 Source: BCG analysis

THE BOSTON CONSULTING GROUP

## Current mitigating measures

Telenor Sweden has taken a number of measures to build resilience and mitigate online risks for children. Their corporate social responsibility agenda is strongly centered on child online safety and includes several initiatives

- Telenor Sweden are members of the initiative “Surfa Lugnt” (Surf Safely), a collaboration between a number of NGOs, authority bodies and connectivity and content providers. The partners work together to raise parents’ awareness on children’s risks and benefits from use of online resources. This helps parents balance their efforts in monitoring online use and acting as support, while still allowing their children to experience the positive effects of an online life.
- Telenor Surf Academy is an initiative started by Telenor and carried out in cooperation with the public school system. The program focuses on skills training of eighth graders, and is built on the notion that the kids themselves might possess a better knowledge of the internet and social media than their teachers. Participation is free and voluntary, where two students from each participating class is chosen to attend a full day work shop with Telenor and learn about copy right laws, social media use and IT tools in school. After the work shop, the students go back to educate their teachers on these topics, and are encouraged to lecture their class mates and even parents.
- Telenor Sweden is taking an active stance against child pornography through two different initiatives
  - Through cooperation with the police, web sites that are publishing child pornographic material are being effectively filtered out for anyone surfing the web through a Telenor-affiliated ISP. The cooperation follows a model first introduced by Telenor Norway, in which Telenor provides the technical solution for filtering out web pages, and the police keeps an updated data base of illegal pages
  - Telenor Sweden has also initiated cooperation with ECPAT (End Child Prostitution, Child Pornography and Trafficking in Children for Sexual Purposes). This cooperation is manifested both by financial support and raising awareness through an internal ECPAT team
- Finally, Telenor Sweden has cooperated with Red Cross to develop a mobile and online chat application for youth who are in need of someone to talk to. Through their technical expertise in developing these applications, Telenor have contributed to increasing available support for children online

These initiatives collectively draw upon a broad base of mitigation levers, ranging from skills training and support, to monitoring and filtering of illegal content, but with particular emphasis on resilience building. It also reflects the high level of social awareness of this issue that so many stakeholders are active in this field.

Going forward, Telenor Sweden plans to further build on their social responsibility ambitions. A newly conducted national survey on how parents and children are using the internet with their mobile phones and tablets will help increase the understanding of consumer habits and give input to future areas for resilience building.

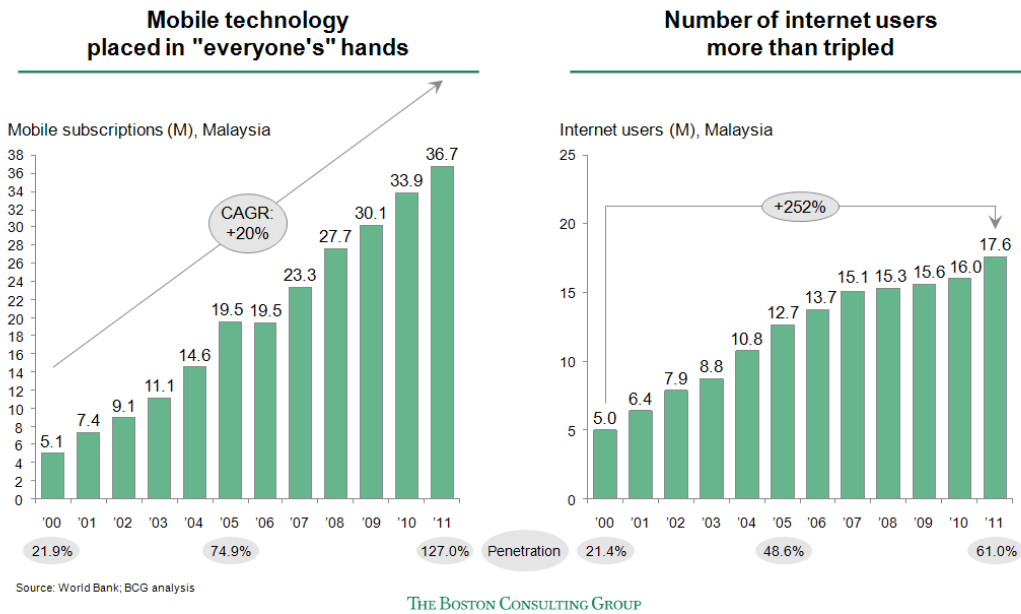




## Malaysia

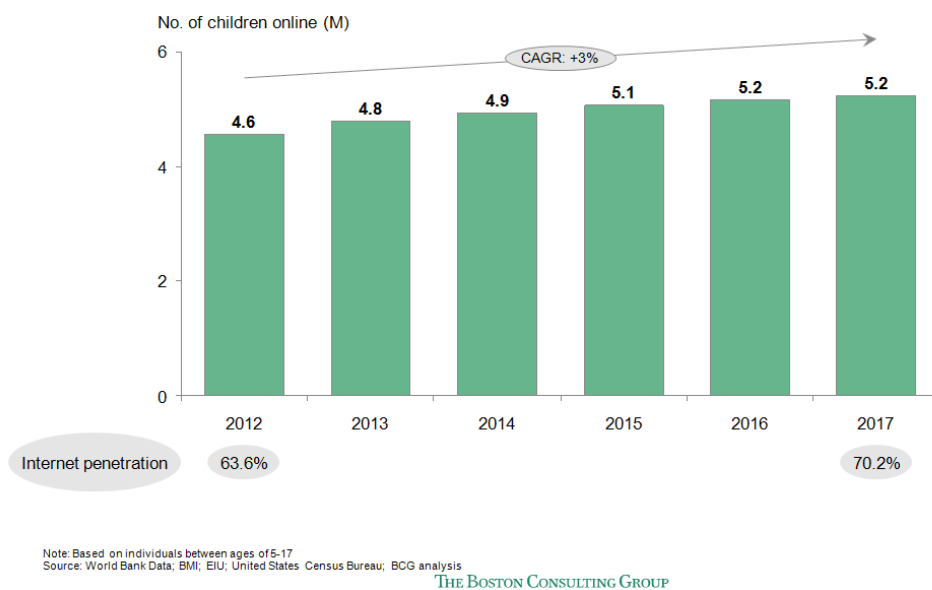
In the past decade, Malaysia has seen a compound annual growth rate of some 20% in mobile subscriptions, with penetration rates rising sharply from about 22% to 127%. In the same period, the number of internet users has more than tripled, rising from 5 million to 17.6 million, with penetration rates increasing from about 21% to more than 61%. By 2017, 700,000 new children are expected to come online in Malaysia, bringing the number of children online to 5.2 million, a compound annual growth rate of 3%, with penetration rising from almost 64% to more than 70%. The country has a medium risk exposure, and a medium level of resilience.

### Malaysia has seen significant increase in access to mobile and online services last decade



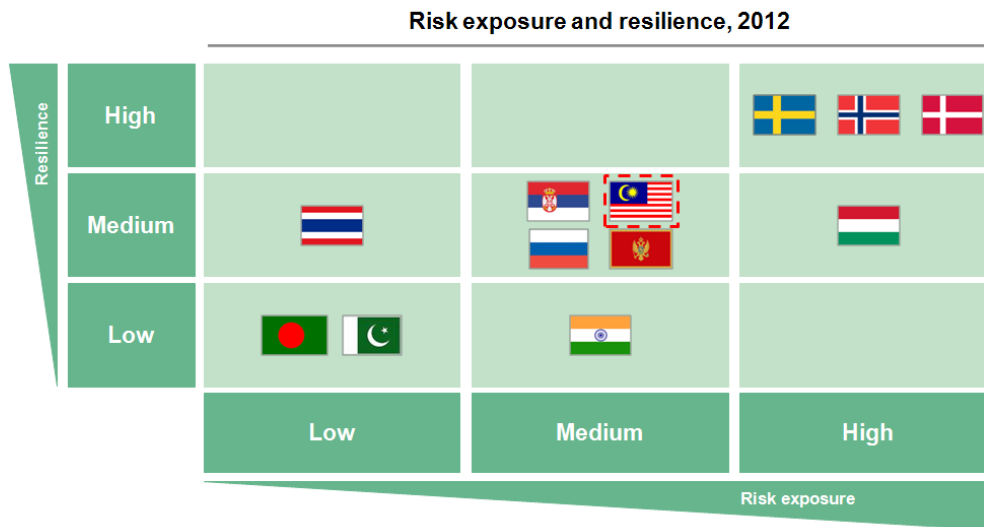
### ~700,000 new children will come online by 2017 in Malaysia

Malaysia expected to reach 5.2 million online children in 2017



## Harm from risk exposure partially mitigated by resilience

Malaysia faces medium risk exposure, and has medium resilience



Source: EIU; ITU; WEF; BMI; World Bank; Communication Chambers; IMF; OpenNet Initiative; Reporters Without Borders; IC Intelligence Center; BCG analysis  
 THE BOSTON CONSULTING GROUP

## Diverse stakeholders must collaborate to succeed

Example stakeholder organizations in Malaysia

<div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Connectivity providers</b></div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Authorities</b></div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Family</b></div> <ul style="list-style-type: none"> <li>Children</li> <li>Parents &amp; other caregivers</li> </ul> <div style="background-color: #e0e0e0; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Ultimate responsibility lies with parents, but other stakeholders need to provide support</b></div>	<div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Content &amp; service providers</b></div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Civil society</b></div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="display: flex; justify-content: space-around; align-items: center; margin-bottom: 10px;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Educators</b></div> <ul style="list-style-type: none"> <li>Schools</li> <li>Youth clubs etc.</li> <li>Community organizations</li> </ul>
--	---

Note: Logo's illustrative of organizations within each stakeholder group – not meant to be exhaustive  
 Source: BCG analysis

THE BOSTON CONSULTING GROUP

## Current mitigating measures

Although internet access has grown rapidly, it is still not ubiquitous in Malaysia. Despite growing concern in some quarters, internet security is currently still not a top priority for the society. Nevertheless, DiGi are already contributing with large initiatives in order to raise awareness and build online skills for the rapidly growing online population.

- The CyberSAFE program is a joint effort between DiGi, various ministries, (such as Cybersafety Malaysia, an agency under the Ministry of Science, Technology and Information, the Ministry of Education, the Malaysian Communications and Multimedia Commission and the Ministry of Women, Family and Community Development) and Childline Malaysia (an NGO), bringing together connectivity providers, civil society, authorities, educators and families. Through a year-long road show (2011-2012), the program visited more than 280 schools and rural internet centers, and reached more than 6800 children and adults, to build awareness and skills on safe use of the internet.
- DiGi's focus for the CyberSAFE program in 2013 is to create a sustainable group of ambassadors consisting of educators, mainly ICT teachers or Digital Resource librarians, from schools nationwide. There will be a greater focus on safety and risks on mobile internet, as well as more digital and e-learning resources made available as toolkits for the ambassadors. The ambassador program includes hands-on training that aims to reach in total more than 45 000 children

The authorities in Malaysia are paying increasing attention to this issue, and have recently launched a large scale internet safety campaign called "Click Wisely" (Klik dengan bijak). The campaign is specifically targeted towards children and parents, with the objective of raising awareness on internet safety and the risks of cybercrime.

DiGi's and the authorities' efforts go a long way towards educating children and their parents on safe internet use, but there is still potential for coordinating and bringing together efforts from authorities, civil societies, connectivity and content providers and educators. As an example, the state government in Terengganu handed out almost 100 000 digital notebook to children, in support of e-learning initiatives, in the last few years before the DiGi CyberSAFE program. The two initiatives complement each other nicely, and increased coordination between such initiatives would greatly benefit all involved.

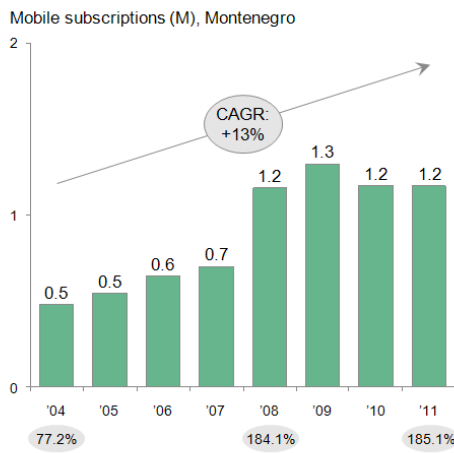


## Montenegro

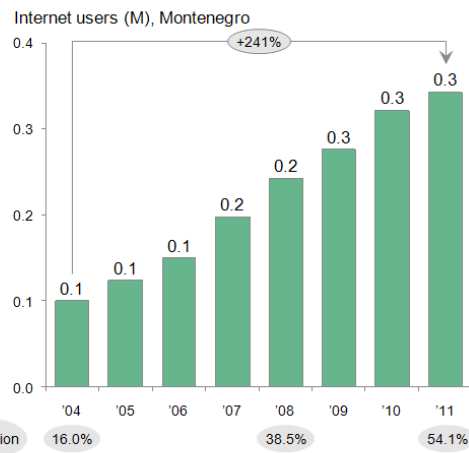
In the past decade, Montenegro has seen a compound annual growth rate of 13% in mobile subscriptions, with penetration rates rising sharply from about 77% to more than 185%. The number of internet users has more than tripled since 2004, rising from 100,000 to 300,000, with penetration rates rising from 16% to more than 54%. By 2017, approximately 5,000 new children are expected to come online in Montenegro, bringing the number of children online to 54,000, a compound annual growth rate of 2%, with penetration rising from more than 57% to almost 66%. The country has a medium risk exposure, and a medium level of resilience.

### Montenegro has seen significant increase in access to mobile and online services last decade

**Mobile technology placed in "everyone's" hands**

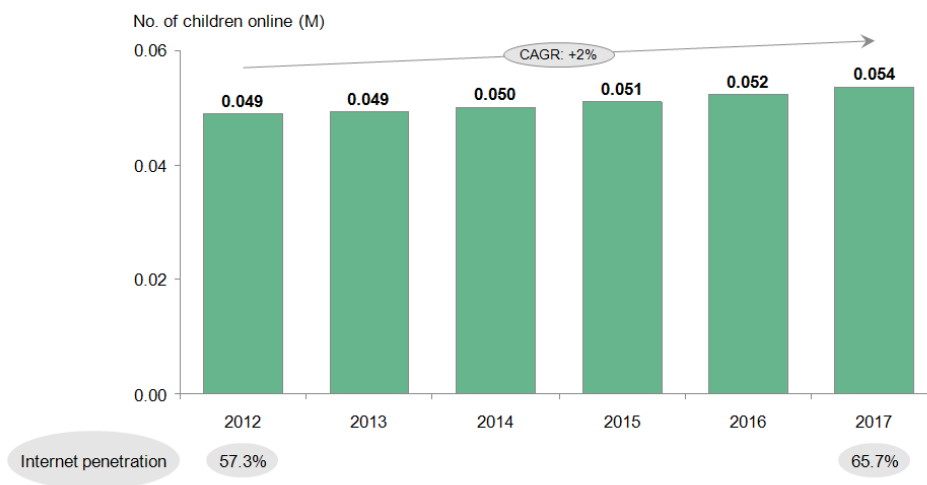


**Number of internet users more than tripled since 2004**



Source: Montenegro Agency for Electronic Communications and Postal Services; World Bank; ITU; BCG analysis  
**THE BOSTON CONSULTING GROUP**

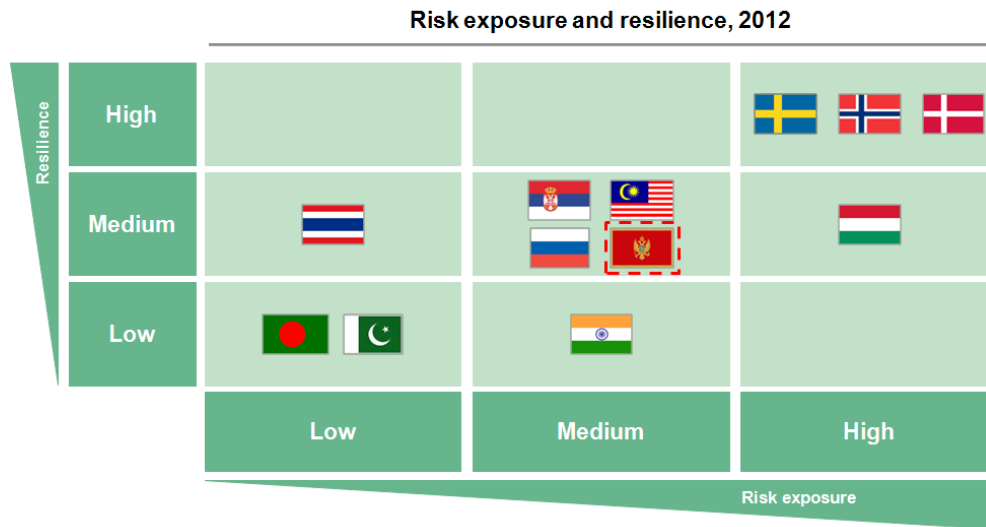
### ~5,000 new children will come online by 2017 in Montenegro Montenegro expected to reach 54,000 online children in 2017



Note: Based on individuals between ages of 5-17  
 Source: Montenegro Agency for Electronic Communications and Postal Services; World Bank Data; BMI; EIU; United States Census Bureau; BCG analysis  
**THE BOSTON CONSULTING GROUP**

## Harm from risk exposure partially mitigated by resilience

Montenegro faces medium risk exposure, and has medium resilience



Source: EIU; ITU; WEF; BMI; World Bank; Communication Chambers; IMF; OpenNet Initiative; Reporters Without Borders; IC Intelligence Center; BCG analysis  
 THE BOSTON CONSULTING GROUP

## Diverse stakeholders must collaborate to succeed

Example stakeholder organizations in Montenegro

<div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Connectivity providers</b></div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Authorities</b></div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Family</b></div> <ul style="list-style-type: none"> <li>Children</li> <li>Parents &amp; other caregivers</li> </ul> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Ultimate responsibility lies with parents, but other stakeholders need to provide support</b></div>	<div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Content and service providers</b></div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Civil society</b></div> <div style="display: flex; justify-content: space-around; align-items: center;"> </div> <div style="background-color: #2e7d32; color: white; padding: 5px; text-align: center; margin-bottom: 10px;"><b>Educators</b></div> <ul style="list-style-type: none"> <li>Schools</li> <li>Youth clubs etc.</li> <li>Community organizations</li> </ul>
--	--

Note: Logo's illustrative of organizations within each stakeholder group – not meant to be exhaustive  
 Source: BCG analysis

THE BOSTON CONSULTING GROUP

## Current mitigating measures

Telenor Montenegro can be considered a frontrunner in pushing the child internet safety agenda in Montenegro, and their initiatives have united efforts from other stakeholders such as the authorities and NGOs. They are involved in a number of programs designed to increase resilience and mitigate online risk for their large population of digitally literate children.

- Telenor Montenegro is taking an active stance against child pornography through cooperation with the Montenegrin Interpol. Web sites that are publishing child pornographic material are being effectively filtered out for anyone surfing the web using Telenor as an ISP. The cooperation follows a model first introduced by Telenor Norway, in which Telenor provides the technical solution for filtering out web pages, and the police keeps an updated data base of illegal pages and operates a consumer hotline
- The pilot project on “Connecting Generations” in 2011 was a success, and is now being followed up with a second round. Bringing together Telenor, the Ministry of Information Society and Telecommunications, the Ministry of Education as well as a parenting organization, this project aims to build awareness and safe internet skills. Focused on children aged 11-13, ambassadors from several schools are chosen to receive workshop-based education on internet safety and then facilitate competitions and sharing of knowledge with their peers in a peer education process. The project trained 20 ambassadors, reaching in total more than 1000 children in five different elementary schools in its pilot phase
- As part of the “Connecting Generations” project, Telenor hosted a safe internet forum, inviting NGOs, government, industry and students to hear about the results, further raising awareness and building support for the safe internet cause
- Building on the success of the “Connecting Generations” project, a second phase, named “Project Conquer Internet, Surf Wisely”, was initiated in late 2012. This phase extends the cooperation with the authorities and the NGO “Parents”, educating 60 Safe Internet Ambassadors in 25 schools, reaching around 4000 pupils and increasing the engagement from parents. Social media has also been utilized in order to raise awareness of the project

Telenor Montenegro has been successful in establishing cooperation with the authorities and acting as a catalyst for the agenda for children’s online safety. The efforts have moved from risk reduction to resilience building, and have helped build awareness in users and stakeholders.



## Building Digital Resilience – Bibliography

### Key books and articles

- Business Monitor International, *Serbia Telecommunications Report (2009)*
- Business Monitor International, *Serbia Telecommunications Report (2013)*
- Business Monitor International, *Bangladesh Telecommunications Report Q1 (2013)*
- Cheon, *Children's exposure to negative Internet content: effects of family context (2005)*
- Childnet International, *Promoting the voice of the child in a digital world: Incorporating 2007-08 accounts (2009)*
- Communication Chambers, *Broadband Pricing Database (2012)*
- d'Haenens et al., *How to cope and build online resilience (2013)*
- eNACSO, *The Next Click: Moving towards a better and safer online environment for every child (2012)*
- European Commission, *European Strategy for a Better Internet for Children (2012)*
- European Commission, *Report of mid-term review meeting of the CEO coalition to make the internet a better place for kids (2012)*
- Finkelhor, *Some Contrarian Hypotheses about the Internet and Youth Safety (2012)*
- Gilligan, *Beyond permanence? The importance of resilience in child placement practice and planning (1997)*
- Ins@fe, *Annual Report 2011 (2011)*
- Ins@fe, *Safer Internet Forum 2012 report (2012)*
- ISTTF, *Enhancing Child Safety & Online Technologies: Final report of the Internet Safety Technical Task Force (2008)*
- ITU, *Child Online Protection: Statistical Framework and Indicators 2010 (2010)*
- ITU, *Guidelines for Industry on Child Online Protection (2009)*
- ITU, *Guidelines for Policy Makers on Child Online Protection (2009)*
- ITU, *Measuring the information society (2011)*
- ITU, *The World in 2011, Facts and Figures (2011)*
- ITU, *Use of information and communication technology by the world's children and youth (2008)*
- Kolpakova, *Understanding risky online behavior of 14-17 years old Russian children (2012)*
- Livingstone et al., *EU Kids Online final report (2011)*
- Lobe et al., *Cross-national comparison of risks and safety on the internet (2011)*
- Livingstone and Hasebrink, *Risks and opportunities on the internet: The perspective of European children (2011)*
- Louge, *Adolescents and the Internet (2006)*
- Medietilsynet, *Barn og digitale medier 2010: Fakta om barn og unges bruk og opplevelse av digitale medier (2010)*
- Medietilsynet, *Barn og medier 2012: Fakta om barn og unges (9-16 år) bruk og opplevelser av medier (2012)*
- Medietilsynet, *Småbarn og medier 2012: Fakta om mindre barns (1-12 år) bruk og opplevelser av medier (2012)*
- Newman and Blackburn: *Report for the Scottish Executive Education and Young People Research Unit: Transitions of Young People: Resilience Factors (2002)*
- OECD, *The Protection of Children Online: Recommendation of the OECD Council - Report on risks faced by children online and policies to protect them (2012)*
- O'Neill et al., *EU Kids Online: Final recommendations for policy, methodology and research (2011)*
- OSTGW, *Youth Safety on a Living Internet: Report of the Online Safety and Technology Working Group (2010)*
- Safer Internet Programme, *Benchmarking of parental control tools for the online protection of children: SIP-Bench II - Assessment results and methodology 4th Cycle (2012)*
- Tstsika et al., *Research on Internet Addictive Behaviours among European Adolescents (2012)*

UNESCO, *Policy Brief: Digital literacy in education (2011)*

UNICEF Innocenti Research Center, *Child Safety Online: Global challenges and strategies (2011)*

World Economic Forum, *Global Competitiveness Report 2012-2013 (2012)*

Wynne and Cooper, *Digital Inclusion Imperatives Offer Municipalities New Social and Economic Opportunities (2007)*

Youth Protection Roundtable - Stiftung Digitale Chancen, *YPRT Toolkit (2009)*

## Primary websites and other resources

Barnevakten: <http://www.barnevakten.no/>

Benchmarking of parental control tools for the online protection of children - SIP-Bench II: <http://sipbench.eu/>

Bruk Hue: <http://www.brukhue.com/>

Economist Intelligence Unit : <http://www.eiu.com>

Eurostat database: <http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/>

GRID - Global Resource & Information Directory: <http://www.fosigrid.org>

Informa - Telecoms and Media: <http://www.informatandm.com/ic/>

International Monetary Fund - World Economic Outlook Database:  
<http://www.imf.org/external/pubs/ft/weo/2012/02/weodata/index.aspx>

International Telecommunications Union: <http://www.itu.int>

Montenegro Agency for Electronic Communication and Postal Services: <http://www.ekip.me/eng/>

OpenNet Initiative: <http://opennet.net/>

Post- og teletilsynet - Telepriser.no: <http://telepriser.no>

Redd Barna Nettvett: <http://nettrett.reddbarna.no>

Reporters Without Borders - Press Freedom Index 2011-2012:  
<http://en.rsf.org/press-freedom-index-2011-2012,1043.html>

Surfa Lugnt: <http://surfalugnt.se/>

United States Census Bureau: <http://www.census.gov>

UN Population Division: <http://www.un.org/esa/population/>

World Bank - Worldwide Governance Indicators: <http://info.worldbank.org/governance/wgi/resources.htm>

World Bank Database: <http://data.worldbank.org/>

World Economic Forum: <http://www.weforum.org/>

You Decide campaign: <http://www.dubestemmer.no/en/>