AGENDA

New Implications of Information Age

Intel and Education

What we are doing in this space
Implications and Actions
Trends That Are Shaping Our World

The Internet Is Growing Up
Reaching The Next Five Billion.. With New Risks

internet.org frames access to the Internet as a human right

2.7B
people online

6.8B
mobile connections

100M
Facebook feature phone users/month

Impact on Systems - The Snowden Effect

**Consumer Perception of Government Data Collection**
- Collecting phone calls & emails?: 63% YES
- Using this data for other purposes?: 70% YES

**Government Policies Focus**
- "The EU could seize 25% of Google’s profits if it violates your privacy.”
  - (Quartz.com, Oct, 2013)

**Emerging New Threats**
- The use of the Internet for terrorist purposes

**Regulation**
- "The EU could seize 25% of Google’s profits if it violates your privacy.”
  - (Quartz.com, Oct, 2013)
More Impact on Individuals
Cyber bullying, Cyber Theft, Digital identity, Privacy, IP

SINGAPORE: About one in four students in Singapore is a victim of cyberbullying, and counsellors fear that many more cases go unreported.


Target data theft: worrying sign of cyber thieves' sophistication

Target Corporation confirmed Thursday that cyber thieves stole credit and debit card data belonging to about 40 million customers who used those cards at its stores nationwide beginning around Thanksgiving and through mid-December.

http://www.carnegiecyberacademy.com/facultyPages/communication/identity.html

Managing Your Online Identity

Your online identity is an ever-changing thing so you have to pay attention to it and make sure it's working for you, not against you. A well-maintained online identity can give people a really good impression of you and open doors to a positive future.

http://www.fbi.gov/about-us/investigate/white-collar/ipr/ipr

Online privacy fears are real
More people are tracking you than you think
## Digital Detox: An Increasingly Common Response

<table>
<thead>
<tr>
<th>Year</th>
<th>% of global consumers who feel stressed</th>
<th>% of global consumers who want to cut down on social networking</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>38%</td>
<td>34%</td>
</tr>
<tr>
<td>2013</td>
<td>43%</td>
<td>45%</td>
</tr>
</tbody>
</table>

Source: GFK Reports Worldwide 2009 and 2013
An ever-connected cyber society demands greater Responsibility to be exercised by all Netizens, in the use of Digital Technologies.
The Digital Divide: How the Online Behavior of Teens is Getting Past Parents (A study by McAfee - a Intel Company)

70% of Teens have hidden their online behavior from their parents, \(\uparrow\) 45% in 2010.
- Half of teens said they would change their online behavior if they knew their parents were watching.

HOW –

- Clearing the browser history (53%)
- Close/minimize browser when parent walked in (46%)
- Hide or delete IMs or videos (34%)
- Lie or omit details about online activities (23%)
- Use a computer your parents don’t check (23%)
- Use an internet-enabled mobile device (21%)
- Use privacy settings to make certain content viewable only by friends (20%)
- Use private browsing modes (20%)
- Create a private email address unknown to parents (15%)
- Create duplicate/fake social network profiles (9%)
Maintaining a Parallel Identity - What is at Stake...?

- **Friendships** - 20% said they had ended a friendship with someone because of something that happened on a social network.

- **Physical Safety** - 7% responded fearing for their safety because of something that happened online, and 5% reported getting into a physical fight because of an online problem.

- **Crime Record** - Surprisingly, 15% report they have hacked someone’s social network account, 31% reported pirated movies and music and 8.7% have hacked someone’s email online.

- **Education** - 16% of teens having admitted to looking test answers on their phone, and 48.1% of teens having looked up assignment and test answers online.

- **Innocence (Pornography)** - 36% have access sexual topics online, and 32% have accessed nude content or pornography online.

- **Bullying** - 62.1% of all teens have witnessed cruel behavior online and 23.3% have claimed to be targets of cyber bullying. 9.5% of teens actually bullying, and 24.9% posting mean comments.
It starts with Education

That brings responsibility & ownership
Our vision
Advance excellence in education worldwide

Our mission
Create and extend computing technology to enrich the lives of every student on earth this decade
Intel Education

We are deeply committed to achieving our shared goals

150M students have used Intel solutions for learning
Transforming education in 100 countries
Professional development for 11M teachers
7M students in Intel Intl. Science & Engineering Fair affiliated fairs
4M employee volunteer hours for education
$1B invested in the last decade

Source: Intel
Our Approach: People Transform Education

Working together, we can achieve our common aspirations
So what are we doing?
Advocacy, Alliances & Education around the world

StaySafeOnline.org
Powered by National Cyber Security Alliance

I WANT TO
Stay Safe Online
Teach Online Safety
KEEP MY Business Safe Online
GET INVOLVED

RESPECTING PRIVACY
SAFEGUARDING DATA
ENABLING TRUST
Data Privacy Day is held every year on January 28.
So what are we doing?
Intel Cyber Security Awareness Pledge & Take Home Kit

- Be more aware of online predators, cybercriminals, and hackers and learn why Internet security is crucial.
- Know how to create secure passwords for devices and online accounts, and how to keep those passwords guarded.
- Know how to selectively disable location settings on devices that can be too revealing.
- Know how to keep important information private online such as addresses, birthdates, full names, social security numbers, etc.
- Pledge to strive for a more secure online world by spreading helpful tips about Internet security to family and friends.
Intel & UNESCO in India: Connecting Stakeholders, Creating Ecosystem

Policy Makers /MoEs /Boards of Education /Advocates
- Cyber safe Standards, Framework for integration

Schools
- Guidelines for ICT practices with cyber safety regulations

Teachers /Counsellors/ NGOs/ Facilitators
- Cyber Wellness Curriculum (Intel India – UNESCO New Delhi Project 2013)

Students
- Awareness Campaigns - Presentations, Awards, Games, Quizzes

Parents
- A 10 Step Internet Safety Plan for your family (McAfee)

*https://sites.google.com/site/cybersafety4adolescents/home
## Security & Privacy Curriculum for Higher Education

<table>
<thead>
<tr>
<th>Problem we are solving</th>
<th>Develop a pipeline of capable students for Intel and our ecosystem who understand security challenges and how Intel technology helps solve those questions.</th>
</tr>
</thead>
</table>
| **Program Results so far...** | • 33 faculty sponsored since 2011 (17 US, 9 China, 7 EU and 1 Brazil)  
• 2500 undergrad students educated in the US and over 3500 WW Sponsored Security Curriculum.  
• Led the Industry/Government/Academe effort to revise the ACM CS2013 standard for security curriculum. Over 90% of the recommendations were accepted by the ACM.  
• Serving as an invited co-chair for a NSF steering committee to host a workshop of academics to identify novel approaches for increasing cyber security education in academia, and developing a standard scale of practice for cyber security education.  
• The Intel sponsored Georgia Tech security pilot program is touching every CS undergrad student (approx. 1300/yr) within the School of Computer Science. |
| **Scaling Plans...** | • An NSF co-funded micro-grant program was started to disseminate Intel supported exemplar curriculum to state and community colleges.  
• Developing 6 Intel educational videos to be used in the classroom setting. |
| **Expected future impact....** | • Students graduating (globally) from schools will have a better understanding of security concepts which will ensure properly educated talent for Intel and technology ecosystem. |
Also Making Security Technologies Available To All – For Safer Digital Life

- **Anti-Malware**: Malware finds nowhere to run or hide
- **Recovery**: Always updated resilient systems
- **Identity**: Simple access with enhanced security
- **Data Protection**: Data safe from theft or alteration

Software and services that use Intel security features benefit from improved prevention and remediation of security vulnerabilities.
Intel’s Five Irrefutable Laws of Information Security

Information wants to be free
- People want to talk, post, and share information – and they increase risk by doing so

Code wants to be wrong
- We will never have 100 percent error-free software

Services want to be ON
- Some background processes always need to be running and can be exploited by attackers

Users want to click
- People naturally tend to click when they see web links, buttons, or prompts. Malware creators know this and take advantage of it

Even a security feature can be used for harm
- Security tools can be exploited by attackers, just like other software. This means that laws 2, 3 and 4 are also true for security capabilities.

Information Age demands responsible behavior and usage of ICT
Call to Action

✓ All stakeholder involvement, awareness & capacity building is key:
  ▪ Students, Teachers, Academia, Parents,
  ▪ Industry, Businesses, Media, Government

✓ Need clear & comprehensive Standards and Policies for “Cyberwellness in Education” that are understood and implementable.
  ▪ Incorporate newer themes like Education governance with open & big data, Education Cloud management etc
  ▪ Security, Privacy, Ethics, Identity aspects are critical for Smart Digital Life (incl addressing cyber bullying, safety, life long identity management etc)

✓ Urgent Education Action Plan at all level for responsible behavior promotion

✓ Security Technology should be leveraged completely for safe usage of ICT everywhere
Thank You
New Cyber Threats

What changes to threats does McAfee Labs expect in the coming year? We foresee several new scenarios as well as some significant evolutions in even the most established threat vectors:

- Industrial threats will mature and segment
- Embedded hardware attacks will widen and deepen
- Hacktivism and Anonymous will reboot and evolve
- Virtual currency systems will experience broader and more frequent attacks
- This will be the “Year for (not “of”) Cyberwar”
- DNSSEC will drive new network threat vectors
- Traditional spam will go “legit,” while spearphishing will evolve into the targeted messaging attack
- Mobile botnets and rootkits will mature and converge
- Rogue certificates and rogue certificate authorities will undermine users’ confidence
- Advances in operating systems and security will drive next-generation botnets and rootkits

Cyber Bullying

“Cyber bullying” is defined as a young person tormenting, threatening, harassing, or embarrassing another young person using the Internet or other technologies, like cell phones.

The psychological and emotional outcomes of cyber bullying are similar to those of real-life bullying. The difference is, real-life bullying often ends when school ends. For cyber bullying, there is no escape. And, it’s getting worse. Read on to get the facts.

1. Nearly 43% of kids have been bullied online. 1 in 4 has had it happen more than once.
2. 73% of students report seeing frequent bullying online.
3. Over 80% of teens use a cell phone regularly, making it the most common medium for cyber bullying.
4. 68% of teens agree that cyber bullying is a serious problem.
5. 81% of young people think bullying online is easier to get away with than bullying in person.
6. 90% of teens who have seen social-media bullying say they have ignored it. 64% have seen others tell cyber bullies to stop.
7. Only 1 in 10 victims will inform a parent or trusted adult of their abuse.
8. Girls are about twice as likely as boys to be victims and perpetrators of cyber bullying.
9. About 56% of kids admit someone has said mean or hurtful things to them online. More than 4 out 10 say it has happened more than once.
10. About 73% have visited a website bashing another student.
11. Bullying victims are 2 to 9 times more likely to consider committing suicide.