IBM **Center for Applied Insights**

Cybersecurity education for the next generation

Advancing a collaborative approach

In a world of increasing information security threats, academic initiatives focused on cybersecurity are proliferating – yet, there is still the danger of falling short in addressing the long-term threat. To avoid becoming too focused on near-term issues, academic programs must be more collaborative across their own institutions, with industry, government and among the global academic community. Only by working in concert can we meet today's demand while educating the next generation to create a more secure future.

About the study

To understand how cybersecurity academic programs, throughout the world, are evolving – and in the process identify both challenges and emerging leading practices – IBM interviewed faculty members and department heads from 15 programs in six different countries. Study participants were selected from over 200 programs followed by the IBM Cyber Security Innovation initiative. To fairly represent a diversity of perspectives, we selected programs from various geographies with varying levels of maturity.

Understanding the need

The number of cybersecurity-related academic programs around the world – whether called information assurance, security engineering or information security – has increased significantly over the past decade. One reason for this growth is the very strong demand from industry and government for trained professionals as both groups are facing a significant skills gap. In fact, over half of industry respondents in a recent survey said that they had too few information security workers on staff.[1] A UK government report said that it may take 20 years to address current and future information and communications technology (ICT) and cybersecurity skills gaps.[2]

To rectify this situation, governments have launched a number of programs, working with industry and academia, to encourage more professionals to enter the cybersecurity field. In the United States, over 160 academic programs have been certified as National Security Agency/Department of Homeland Security National Centers of Academic Excellence in Information Assurance.[3] Meanwhile, in India, the University Grants Commission has asked that cybersecurity be introduced at both the undergraduate and post-graduate levels nationwide, based on a task force recommendation.[4]

Government and industry are creating demand, but what's the view of students and educators when it comes to security? Over 450 students and 250 educators in computer science, information systems and engineering participated in the latest IBM Tech Trends research and shared their opinions on emerging technology areas.[5] Both groups see security as extremely important, with 56 percent of students and 44 percent of educators ranking it as one of the top three issues the IT industry will face over the next two years. When asked what they saw as the primary barriers to the adoption of mobile, cloud computing and social business, security came out on top.

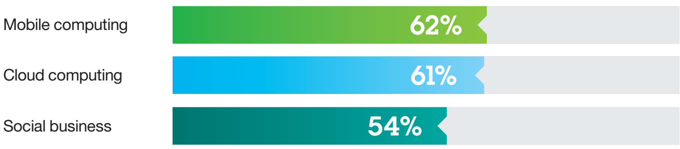

Figure 1 – Percentage of students and educators who see security as a top barrier to technology adoption

These key stakeholders clearly see security as a critical issue, but do they feel their programs are addressing it? Less than 60 percent of the students and educators surveyed believe their academic programs address the creation and development of IT security practices for these emerging technology areas.

These findings suggest that, despite the progress being made, work still needs to be done. Educational institutions need to do more to fully embed information security practices and principles into academic programs.

Understanding the trends

Four common trends were identified by the educators we interviewed. The first is that *information security is increasing in relevance.* No longer just a highly specialized area, it is something that impacts people every day. In an interconnected world reliant upon smart phones, social media, e-commerce and cloud services, information security impacts more and more of the public. It has become personal.

The second trend *is increasing attention and demand from students, private industry and government agencies.* More and more industries, from banks and financial services companies to aerospace and defense firms, as well as healthcare providers are seeking graduates with specialized security skills. Training an expert cybersecurity workforce is now a national priority for many countries. Those interviewed said that almost all of their students are hired after graduation. Some are hired even before they graduate and finish their degrees while working. Rising demand is prompting the creation of more programs at the university, community college and vocational levels–all of which compete for talent and resources.

Thirdly, the field of cybersecurity has also significantly expanded with *more domains to secure and more ways to attack.* This means more to teach and to learn. Today, attacks are extremely hard to detect; attackers are stealthier and more evasive. In response, academic programs are expanding beyond traditional areas like cryptography, and countering sniffing and denial of service attacks. Cybersecurity education now covers new areas like cyber-physical attacks, the protection of heterogeneous systems and real-time security data analysis.

Lastly, academic programs are moving away from teaching purely the principles and theory of security to *focus more on the practices.* This is largely driven by the demands of industry and governments, as well as by students who want to focus more on real-world problems and practical challenges.

Straining to address the needs and trends

High demand, growth in the number of programs, increased threat and expanding domain are combining to create a number of challenges for educators. This puts a strain on both organizational and technology resources.

The main difficulty for university programs is *finding qualified instructors and professors*, especially junior faculty. Industry and government are recruiting highly skilled cybersecurity experts at a rapid pace and draining the pool of potential faculty. The level of worldwide competition for talent is also rising sharply as the number of academic programs grows. Some of the non-U.S. universities we interviewed to said it was particularly hard to retain faculty over the long term, with some professors leaving after only a couple of years for opportunities in the United States.

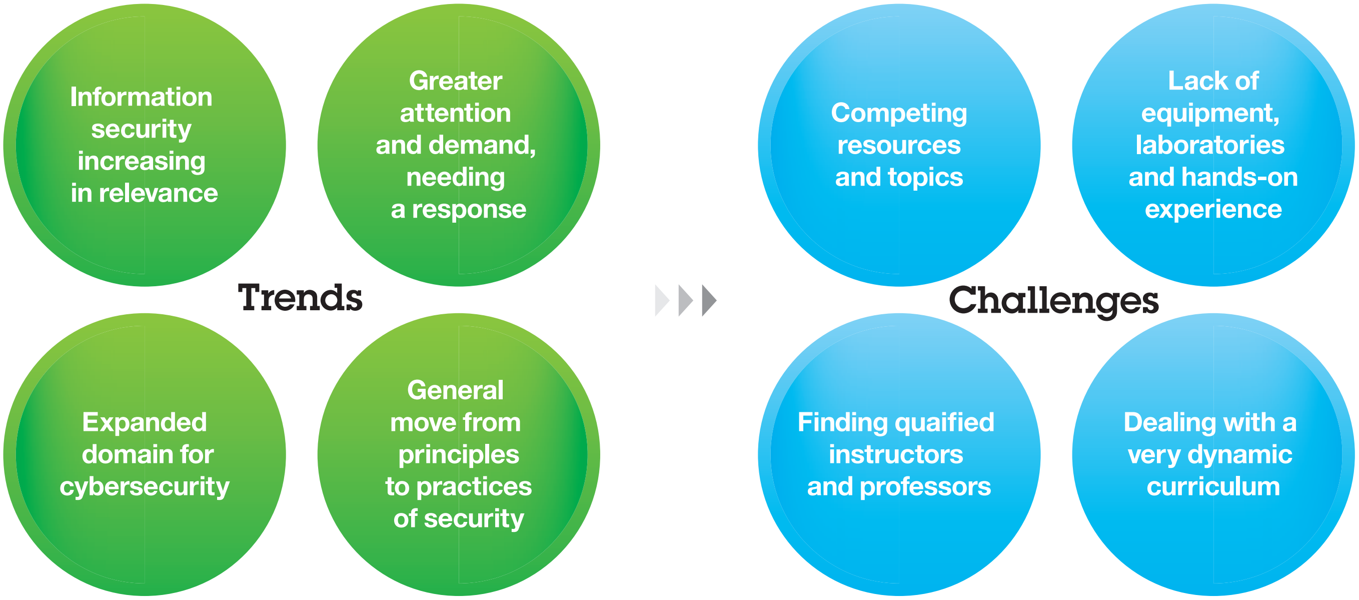
Information security increasing in relevance
Greater attention and demand, needing a response
Trends
Expanded domain for cybersecurity
General move from principles to practices of security
Competing resources and topics
Lack of equipment, laboratories and hands-on experience
Challenges
Finding quaified instructors and professors
Dealing with a very dynamic curriculum

Figure 2 – Trends and challenges in cybersecurity education

Institutions are also *struggling for resources with competing subjects*. A number of the programs we looked at draw professors from multiple departments. Departments have competing priorities and limited faculty slots, and they are not solely focused on cybersecurity. For example, a cybersecurity program based in the computer science department must contend with other important emerging topics such as mobile technology, cloud computing and analytics.

Another major challenge is a *critical lack of equipment, laboratories and opportunities for students to get hands-on experience*. Many of the faculty we spoke to use either open-source tools or their own internally developed software and simulators. Even when programs receive a donation, the budget for training and maintenance isn't there. Students need access to state-of-the-art, easy-to-use test beds, simulation tools and training networks. They should focus on learning principles instead of complex tools.

A very *dynamic curriculum* is putting added pressure on cybersecurity professors and programs. As threats evolve rapidly and continuously, it is difficult to stay aligned with the latest solutions and technologies. In general, classes need updating every year, requiring time and resources that are hard to come by. With the ever-widening purview of cybersecurity (for example adding cyber-physical infrastructure, healthcare, legal and policy issues to the mix), this issue isn't going away anytime soon.

> *"Similar to the observation that security must be built into systems from the start, security concepts also need to be covered in the computer science curriculum from the very beginning…this creates the challenge of making room for these concepts in courses that already have plenty of material in them."*
>
> — Dr. Mustaque Ahamad
> Professor, College of Computing, Georgia Institute of Technology

Different approaches, common ground

In response to these trends and pressures, academic institutions are taking different approaches to cybersecurity education. Some believe in specializing early and focus more on the application of cybersecurity, making it a part of mainstream undergraduate education. Others aren't advocates of specialized undergraduate degrees and think it is more important to have a strong grounding in the fundamentals of computer science first. While opinions differ, it is important to highlight the debate so common ground can be found.

Common themes emerged during our interviews:

- Cybersecurity must evolve into a formal discipline in the curriculum similar to other existing disciplines.
- Programs must teach a combination of theory and practice.
- Cybersecurity should be taught in an integrated fashion, with all students learning basic principles.
- Independent study and student interest groups are a key teaching tool.
- Government and industry collaboration is extremely important.
- Providing strong faculty development opportunities is a must.

Linking efforts at all levels

Any one academic program cannot, on its own, address the full range of trends, challenges, issues and differing perspectives. There is a clear need for leading practices that promote a collaborative approach and a longer-term focus.

Seven different tenets for cybersecurity education surfaced during our interviews. Together, they can serve as guidance in the development of new capabilities. The principles fall into three groups, all focused on collaboration – within institutions, with industry, government and across the global academic community. No single program had all of these characteristics.

Collaborate within your own institution

- *Holistic* – A comprehensive approach from a technical perspective is essential. Designing and managing security for networks, software, hardware, data and applications is crucial. The majority of existing programs provides a broad spectrum of courses, covering both traditional security (e.g., cryptography) and emerging technical areas (e.g., mobile and cloud security). Almost all of the programs require some education in ethics. Many also cover the legal, business, government and social issues associated with cybersecurity.

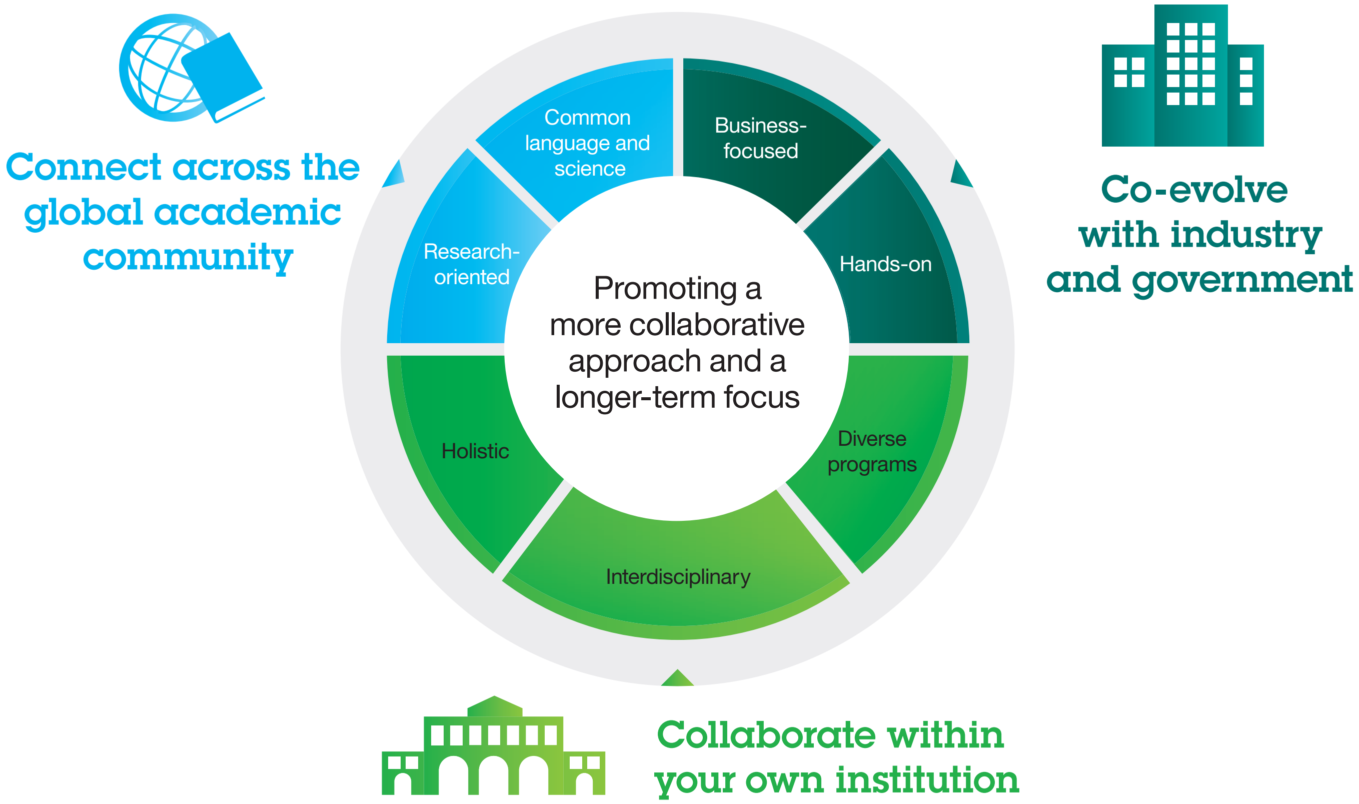
Connect across the global academic community
Common language and science
Business-focused
Co-evolve with industry and government
Research-oriented
Hands-on
Promoting a more collaborative approach and a longer-term focus
Holistic
Diverse programs
Interdisciplinary
Collaborate within your own institution

Figure 3 – A unifying set of leading practices

- *Interdisciplinary* – Institutions are beginning to work across academic disciplines to incorporate cybersecurity into non-technical academic programs. Although interdisciplinary efforts are in their infancy, a few are in the planning and development stages. These include joint programs with business, medical, law, economics, public policy, criminology and even journalism schools.
- *Diverse programs* – Most educators we interviewed have programs at the Master's and Ph.D. level and a few have dedicated undergraduate programs. Almost all had different approaches based on whether cybersecurity is taught as part of engineering or computer science. Concentrations, minors, post-graduate certificates and professional development programs in cybersecurity were also popular.

> *"Interdisciplinary education for cybersecurity is essential. It is not only about computer science and engineering. We are working to bring together multiple programs from our university–criminology, brain sciences, statistics, ethics, healthcare informatics, economics and risk analysis–to truly develop a comprehensive approach to security thinking."*
>
> — Dr. Bhavani Thuraisingham
> Louis A. Beecherl Jr. Distinguished Professor, Department of Computer Science,
> Executive Director of the Cyber Security Research and Education Institute,
> The University of Texas at Dallas

Undergraduate specialization

The Computing Security BS degree program at the Rochester Institute of Technology was launched over six years ago. This was in a response to faculty recognition of a growing need for security professionals that would continue to increase for many years to come. With feedback from our Industrial Advisory Board, we created a dynamic and evolving curriculum that addresses the many aspects of security theory, reinforced by experiential and co-operative learning experiences. Through the use of extensive laboratory work in combination with required co-operative work experiences, graduates achieve mastery not only in computing security theories but also develop the capability to apply the theory in practice. After completing core course work that gives them a firm foundation in computing, students select a six-course advanced sequence from a variety of specialty areas such as network security, systems security, digital forensics, malware analysis, secure software development, or computing security theory. Their education is then completed with a senior capstone project. Since the inception of the program, over 200 students have graduated and experienced a very high placement rate. We are still challenged to get more high school students to major in computing security, in order to address the growing need for security professionals.

– Sylvia Perez-Hardy
Associate Professor & Chair, Department of Computing Security, Rochester Institute of Technology

Co-evolve with industry and government

- *Business-focused* – Programs with a strong business focus generally have formalized processes and structures. Most have an industry advisory board or group of sponsors that meet regularly. These business partners tend to be deeply engaged, funding research and design competitions, providing fellowships and scholarships, contributing to curriculum design and sending their own employees to the institution for training and advanced degrees. Programs without extensive business partner involvement still had security professionals giving lectures or hosting industry nights.
- *Hands-on* – Since many programs struggle with a lack of resources to adequately address students' needs, they are coming up with creative solutions. Interviewees stated that extensive lab work and projects, both individual and group, are very important. Some have a dedicated lab class while others rely on lab modules. Special-interest groups such as "grey hat" clubs and hacking competition teams enjoy high popularity. They are sometimes the primary source of practical experience for students despite not always being part of the official curriculum. Another common practice is working with industry and government organizations on co-op programs and internships, some mandatory.

Practical experience

Temasek Polytechnic's School of Informatics & IT provides a hands-on, practice-oriented education, emphasizing the development of problem-solving and thinking skills. The School will be setting up a Security Operations Centre (SOC) as a Learning Enterprise for students from the Cyber & Digital Security and Digital Forensics programs. The SOC is expected to be operational early 2014. It will monitor the School's network of 1,600 students. The unique feature of the SOC is that students will monitor and respond to actual security events and incidents. By combining a hands-on environment with relevant subjects in the classroom, the School believes that its students will acquire knowledge and skills that are industry-relevant and highly valued.

– Ho Hee Meng
Manager, Security & Governance,
School of Informatics & IT, Temasek Polytechnic

> *"We take pride in our close association with industry in building our cybersecurity research and education programs. We can realign our research and curricular focus based on their exposure to the latest trends and needs in the market."*

— Dr. Suku Nair
Professor and Chair, Department of Computer Science and Engineering,
Director of SMU HACNet Labs, Southern Methodist University

Connect across the global academic community

- *Research-oriented* – Dedicated research centers, publications, grants and collaborations are all important parts of a strong research program. Many universities have formal research institutes. In some cases, they are physical locations with labs. In other cases, their role is limited to providing strategic focus and coordinating research opportunities for faculty. Many programs are part of single- and multi-university research initiatives conducted in collaboration with national governments. Some programs yield marketable innovations while others are subject to regulations that prevent the easy commercialization of research. State and national institutes are more interested in fostering economic development in a dedicated way. Most programs see their students as their primary form of technology transfer.
- *Common language and science* – A number of professors and department heads see the need for building a science of security and establishing a cross-discipline *lingua franca* among scientists, engineers and policy makers. For example, government uses the term "cybersecurity" while industry tends to use "information security." The differences extend to definitions as well – some see information security as limited to perimeter protection, while others extend its domain to people, data, networks and applications. A foundation for the science of security is being explored at many universities.

"There is a significant need for a common language of information security, not within the technical discipline, but between government, academia and different industries–information security specialists need to be understood by engineers, policy makers and business leaders, and vice versa."

— Prof. Dr. Michael Waidner
Chair Professor for Security in Information Technology, Technical University of Darmstadt, Director of the Fraunhofer Institute for Secure Information Technology

A science of security

Critical cyber systems must inspire trust and confidence, predictably protect the integrity of data and resources as well as the privacy of data owners, and perform securely, safely, and reliably. Therefore, a scientific basis for the design and analysis of trusted systems is needed. Security science should give us an understanding of the limits of what is possible in some security domain by providing objective and quantifiable descriptions of security properties and behaviors. Security science should have broad applicability, transcending specific systems and not be limited to the current forms of attack and defense. To assist in addressing these challenges, the National Security Agency recently initiated a coordinated set of focused research activities taken under the auspices of three Science of Security Lablets – at the University of Illinois at Urbana-Champaign, North Carolina State University, and Carnegie Mellon University. The Lablets share a broad common goal, which is the advancement of a more scientific approach to security related research, with focus on a selection of the hardest technical problems and research to advance the solution to these problems.

– Laurie Williams, Ph.D.
Professor, Department of Computer Science,
North Carolina State University

Meeting the demands of tomorrow

The trends, challenges, and leading practices uncovered through our interviews show that cybersecurity education programs are entering a period of transformation. Only by working in concert can they meet today's demand while preparing a new generation of professionals for future challenges. The key question is: what needs to be done next?

Our recommendations focus on increasing and improving openness and collaboration, along with addressing both immediate priorities and longer-term strategies. Programs must strive to balance the near-term requirements of industry and government while educating future faculty members and researchers, developing more internships and fellowships, and continuing investments in research.

These are the key initiatives of prime importance in the development of cybersecurity education.

1. *Increase awareness and expertise*– We must all work to raise the level of awareness across the academic community. Cybersecurity is no longer a hidden area embedded in computer science or engineering disciplines. Programs need to graduate more computer scientists and engineers with hands-on training and the ability to design and develop secure systems from the start.
2. *Treat security education as a global issue* – Cybersecurity issues are not relegated to a single country. They know no boundaries. Institutions need to share and collaborate with other programs around the world. Academics from more mature countries should increase their formal collaboration with those in emerging countries to help address the skills gap. Such initiatives could include distance learning programs and the sharing of curriculum and best practices among educators.
3. *Approach security comprehensively, linking technical to non-technical fields* – Adopt a curriculum that has a holistic and interdisciplinary approach. Security education should cover infrastructure, people, data, applications, ethics, policy and legal issues. Business and public policy schools should focus on creating better security policy and governance and training future information security leaders, such as Chief Information Security Officers.
4. *Seek innovative ways to fund labs and pursue real-world projects* – Resources will always be tough to come by. Industry, government and academia must come up with novel ways to give students practical experience. More internships and design contests are one way to overcome this challenge. Other alternatives include cloud-based or virtualized ranges, simulators and test beds.
5. *Advance a "science of security"* – Place emphasis on the creation of a discipline of security science with fundamental concepts and a common vocabulary. This new science should focus on anticipating security problems, not just reacting to attacks. It must include scientific methodologies and incorporate reproducibility and proofs in the design of security systems.

Now is the time to act

We believe that these recommendations offer ways to make cybersecurity education more effective in the short and the long term. By breaking down barriers and working in concert, it is possible to better address current and emerging challenges.

We must maintain our current level of fervor and effort in the field while keeping our eyes on longer-term goals. The academic community will achieve more by collaborating broadly. Governments must invest in programs that advance the science behind cybersecurity, along with fundamental education in science, technology, engineering and mathematics. At the same time, industry must provide technology, opportunity and expertise. It will take all of us to create a more secure future.

What's your view? We invite you to share your own insights and perspectives with us via email at ibmcai@us.ibm.com or Twitter at @IBMCAI.

About the authors

Marisa Viveros is a Vice President at IBM Corporation, leading the Cyber Security Innovation initiative globally. She is responsible for creating education and research programs that foster stronger collaborations among academic institutions, government organizations and IBM to develop cyber and information security knowledge and talent to address the skills shortage. She can be reached at viveros@us.ibm.com.

David Jarvis, Senior Consultant at the IBM Center for Applied Insights, specializes in fact-based research on emerging business and strategic technology topics. In addition to his research responsibilities, David teaches on business foresight and creative problem solving. He can be reached at djarvis@us.ibm.com.

Contributors

We thank all of the academic programs that took the time to share their experiences, insights and opinions to help shape this document.

We acknowledge our team without whose gracious contribution of time and expertise this work would not have been completed:

Dianne Fodell
Sadu Bajekal
Paul Kontogiorgis

About the IBM Center for Applied Insights

ibm.com/ibmcai

The IBM Center for Applied Insights introduces new ways of thinking, working and leading. Through evidence-based research, the Center arms leaders with pragmatic guidance and the case for change.

About IBM Academic Initiatives

ibm.com/university
ibm.com/academicinitiative

The IBM Academic Initiative, part of our University Relations program, offers resources for educators and students in technology areas such as business analytics, big data, mobile computing, cloud computing, and cybersecurity. The resources include training, technology and curriculum materials for faculty along with expanded programs to directly engage students with real-world business challenges.

Notes and sources

[1] *The 2013 (ISC)² Global Information Security Workforce Study.* Frost & Sullivan in partnership with (ISC)² and Booz Allen Hamilton. January 2013. https://www.isc2.org/workforcestudy/Default.aspx

[2] *The UK cyber security strategy: Landscape review.* National Audit Office. February 2013. http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

[3] *Centers of Academic Excellence Institutions.* National Security Agency (NSA) Central Security Service (CSS). http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

[4] "Cybersecurity to be part of India's college, university curriculum." *The Times of India.* January 17, 2013. http://articles.timesofindia.indiatimes.com/2013-01-17/education/36393726_1_cybersecurity-security-scenario-information-security

[5] *Fast track to the future: The 2012 IBM Tech Trends Report.* IBM Center for Applied Insights. December 2012. https://www.ibm.com/developerworks/mydeveloperworks/blogs/techtrends/?lang=en

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
April 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided

Please Recycle