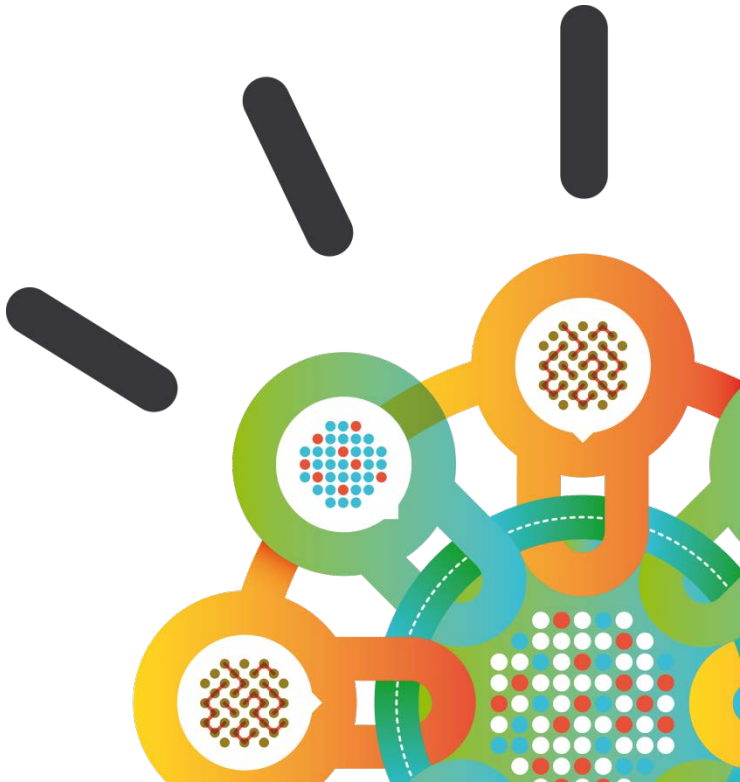
Security Intelligence.
Think Integrated.

Cybersecurity education for the next generation – *Emerging best practices*

Presented at the 2013 NIST/NICE Workshop
Gaithersburg, Maryland

Marisa S. Viveros
Vice President, Cyber Security Innovation
IBM Corporate Strategy
viveros@us.ibm.com



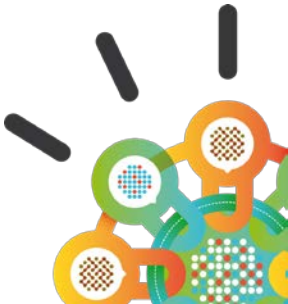
Agenda

1. Cybersecurity is Imperative to Industry

2. Findings from a Cybersecurity Survey

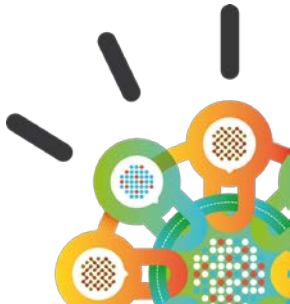
3. IBM Initiatives to Support Cybersecurity Education

4. Concluding Remarks



Agenda

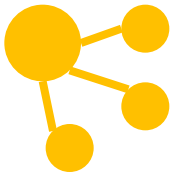
1. Cybersecurity is Imperative to Industry
2. Findings from a Survey to Leading Academics
3. IBM Initiatives to Support Cybersecurity Education
4. Concluding Remarks



Innovative technology changes everything

1 trillion connected objects

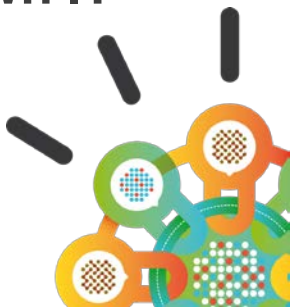
1 billion mobile workers



Social business

Bring your own IT

Cloud and virtualization



Motivations and sophistication are rapidly evolving

National Security

Nation-state actors
Stuxnet

Espionage, Activism

Competitors and Hacktivists
Aurora

Monetary Gain

Organized crime
Zeus

Revenge, Curiosity

Insiders and Script-kiddies
Code Red

Security skills to help manage heightened security risks are difficult to find

58%

are unable to find people with the right skills

53%

enable to measure the effectiveness of their security efforts

66%

struggle with an understaffed IT team

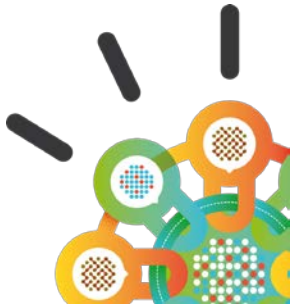
FORRESTER®

81% of chief information security officer functions are re-organizing or have been re-organized ***within the last six months***.

Corporate Executive Board, Information Risk Executive Council Study, July 2012

Agenda

1. Cybersecurity is Imperative to Industry
2. Findings from a Cybersecurity Survey
3. IBM Initiatives to Support Cybersecurity Education
4. Concluding Remarks



Analysis approach

- IBM monitors over 200 cybersecurity academic programs as part of its Cyber Security Innovation program
- From those 200+ institutions, we selected 15 programs in 6 different countries
- The selections were made based on geographic location, program maturity, and diversity of approaches
- We conducted 60 minute qualitative interviews with faculty members, department chairs and others
- We augmented the research with data from IBM's 2012 Tech Trends which surveyed over 450 students and 250 educators from 13 countries

Cybersecurity is top of mind for students, educators, industry and government – *there is a proliferation of programs and a very strong demand for trained professionals*

- Industry and government are currently facing a **significant skills gap**
- There is an **enormous focus** from national governments
- The academic programs we interviewed all stated that the **demand for their students is extremely high**
- In the **future**, our interviewees envisioned:
  - A larger threat
  - Increasing demand and more programs
  - New skills needed and taught
  - More rigor and a broader scope

> *"The DoHS can't find enough people to hire, and there are not enough people in the pipeline to protect companies, critical infrastructures and governments in future… Governments, business and the IT security industry need to work together to make cyber security more visible and attractive as a career."*[1]
>
> - Mark Weatherford, Deputy Under-secretary for Cybersecurity at the US Department of Homeland Security (DoHS)

SOURCES: (1) *"RSA 2013: Cyber security skills shortage needs urgent attention, says DoHS",* ComputerWeekly.com, 2/26/13

Students and educators see security as an important topic – *they also see it as a barrier to technology adoption and feel their institutions aren't doing enough*

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

Less than 60% of students and educators believe their academic programs address the creation and development of IT security practices for these emerging technology areas

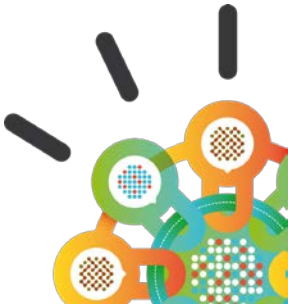
With all of the progress being made by cybersecurity academic programs, there is still work needed to fully embed information security practices and principles

SOURCE: *IBM 2012 Tech Trends*

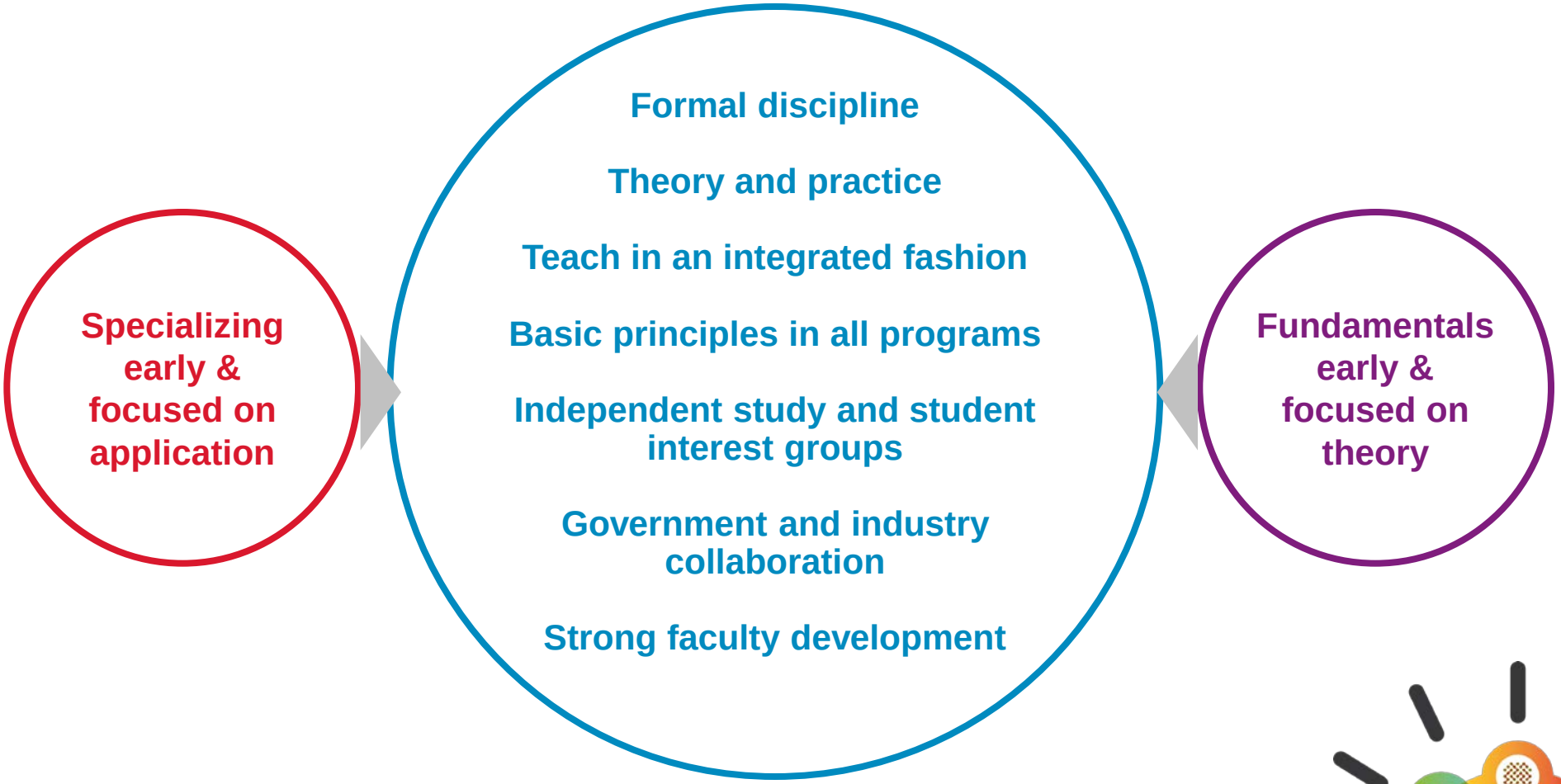
Trends and Challenges

- … *more of everything*
  - Information security increasing in relevance
  - Greater attention and demand, needing a response
  - Expanded domain for cybersecurity
  - General move from principles to practices of security

- … *straining organizational and technology resources*
  - Competing resources and topics
  - Lack of equipment, laboratories and hands-on experience
  - Finding qualified instructors and professors
  - Dealing with a very dynamic curriculum



Programs are addressing the challenges in different ways – *taking different approaches to cybersecurity education, but still sharing common principles*



These trends, challenges, issues and differing perspectives cannot be met by each academic program on its own – *a set of leading practices is needed*

Collaborate within your own institution

Holistic	• Programs provide a broad spectrum of traditional and emerging technical areas • Covers security policy and management
Inter-disciplinary	• Requires an ethics course • Offers courses in policy, management, public policy, international affairs, psychology, law, and economics • Joint programs with other schools
Diverse programs	• Most programs are focused at the graduate level, fewer have dedicated undergraduate programs • Concentrations or minors

"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

Co-evolve with industry and government

Hands-on

- Extensive laboratory work and projects
- Special interest groups, “grey hat” clubs and hacking competitions
- Students as tech support or security operations for university
- Mandatory internships

Business focused

- Formalized processes
- Industry advisory board
- Business partners provide inputs on curriculum design
- Fellowships and scholarships
- Fund research, sponsor design projects and research centers
- Send employees for training and advanced degrees

“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	▪ Formal research institute(s) that are cross-department ▪ Single and multi university research initiatives with national governments ▪ Students are the primary form of technology transfer
Global collabor-ation	▪ Most global collaborations aren ‘t formal ▪ A need for a common language between scientists, industry and policy makers ▪ Need the development of a foundation for the “science of security”

“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

Recommendations

1. Increase awareness and expertise
2. Treat security education as a global issue
3. Approach security comprehensively, linking technical to nontechnical fields
4. Seek innovative ways to fund labs and pursue real-world projects
5. Advance a “science of security”



Strive to balance the near-term requirements of industry and government while educating future faculty members and making investments in research

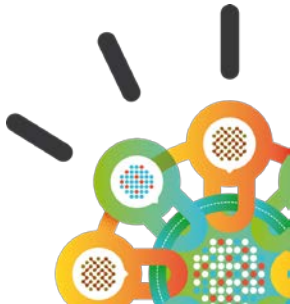
Agenda

1. Cybersecurity is Imperative to Industry

2. Findings from a Cybersecurity Survey

3. IBM Initiatives to Support Cybersecurity Education

4. Concluding Remarks



IBM University Programs

- Research (Collaboration)
- Readiness (Skills)
- Recruiting (Jobs)
- Responsibility (Volunteers)

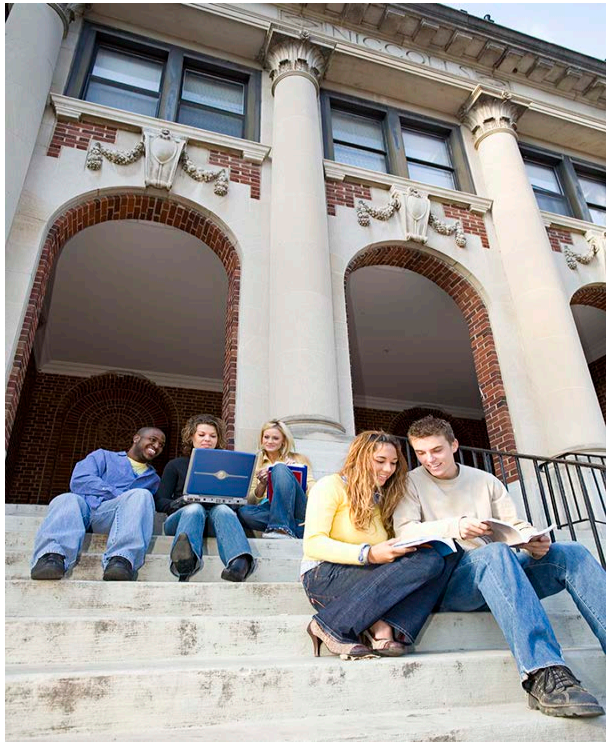
- Regions (Smarter Cities, Startups & Workforce)

The IBM Academic Initiative is designed to grow skills needed to build a Smarter Planet

Since inception in 2004:
37,000 faculty across 13,000+ institutions have participated in the Academic Initiative, teaching 130,000 courses to 3.8M students

- Extensive expertise, capabilities, and community resources to develop world-class curricula
- No charge access to IBM technology & tools
- Real-world cases and experiential learning
- Activities to connect students to an ecosystem of industry partners

ibm.com/academicinitiative



Helping faculty teach skills relevant to high growth market areas where job growth is brisk

Execution framework to build cybersecurity human capital while creating awareness of IBM security capabilities

CAPABILITIES

Securely Provision	Operate & Maintain	Protect & Defend	Investigate	Operate & Collect	Analyze	…

SKILLS TAXONOMY: Security Consultants, Security Architects, Digital Forensic, Security Analysts, etc.

1. PROGRAMS & CERTIFICATIONS
2. IBM SECURITY AMBASSADORS
3. IBM PRODUCTS Red Books Best Practices
4. Faculty Award, SUR, OCR, IDR

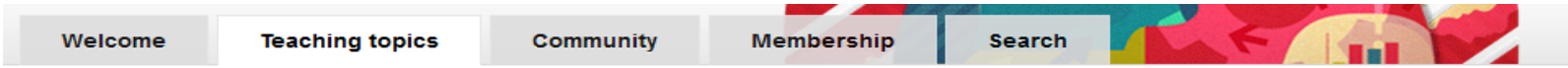
UNIVERSITY PARTNERS

CYBER SECURITY PROFESSIONALS

+

IBM SECURITY BRAND AWARENESS

IBM Academic Initiative website offers software, redbooks and course material to academics



Security and information assurance

Security has ascended in importance across businesses of all sizes, whether it's the CMO evaluating the potential risk to the brand, the CFO understanding the financial implications of adverse events, or the COO assessing the impact of IT systems disruptions on ongoing operations. Developing security intelligence skills — the ability to proactively predict, identify, and react to potential threats — will take on a new priority in the digital age.

We have software, courseware, and other resources for you to use in your classrooms and labs so that your students can get the skills they need to become part of the information security profession.

Security and information assurance focus areas

- **Data protection and access management**
  Learn how to protect information from unauthorized use, disclosure, modification, or destruction and eliminate risks from insecure database configurations.
  Recommended products: InfoSphere Guardium, IBM Security Access and Identity Manager
- **Infrastructure security**
  Teach students how to address security issues across an IT environment to ensure each device is protected from malicious activity.
  Recommended products: IBM Security Server Protection and Virtual Server Protection, IBM Security SiteProtector System
- **Intelligence, analytics, and compliance**
  Show your classes how to gather, analyze, measure and interpret event data from an IT environment to detect malicious activity and demonstrate compliance.
  Recommended product: IBM Security Content Analysis SDK
- **Secure software engineering**
  Ensure your students understand the best practices to use throughout the software development lifecycle to prevent, detect, and eliminate vulnerabilities.
  Recommend product: IBM Security AppScan

Become an Academic Initiative member

→ Join now — at no charge!

→ Renew your membership

Contact IBM Academic Initiative

Email

→ Get support

More resources

- ISACA: Model Curriculum for Information Security Management
- ISACA: Model Curriculum for IS Audit and Control
- US-CERT: Competency and Functional Framework for IT Security Skills

http://www-03.ibm.com/ibm/university/academic/pub/page/security

Security Training Program – *5 day program to train-the-trainers*

Overview

The program is an introduction to information security around a IBM security taxonomy, built with the aid of publications from security related bodies and associations such as ACM, ISC2, NICE and ISACA.

The objective is to introduce the university faculty with the core topics of Information Security, to help them understand the scope and breadth of security measures/controls and management that need to be addressed, risk management and governance models and an introduction to frameworks like ISO27001 and COBIT that oversee the controls.

The content can be leveraged to create coursework in universities under a structured set of foundational core topics and electives.

Offer to those schools making a commitment to IBM by signing agreements to use IBM technology

Syllabus (sample topics)

The role of Security

1.What does it mean to be secured?

2.Principles and concepts – asset protection, confidentiality, integrity, defense-in-depth

3.Risk identification and analysis

4.Security as a business process

5.Security services – authentication, authorization, audit, integrity, non-repudiation

6.Security management – policy management and enforcement, identity assurance.

End-to- end Security

1.Establishment of trust – what does it take?

2.End-to-end security – extend security principles across domains: networks, endpoints, systems, applications, data, people, processes and physical

3.Digital identity – lifecycle management, provisioning, separation of duties, password management, etc.

4.Authentication – basis of authentication, multi-factor, single sign-on, etc.

5.Access control requirements – reliability, consistency, etc.

Application Security

1.Federation scenarios of cross-domain services

2.SOA security – WS-security, identity aware ESB

3.Cryptography – encryption and signing algorithms, certificates, PKI, etc.

4.Policy management – business, architectural and operational

5.Application security – SDLC, secure programming, secure coding practices, software language security support.

Data Security Management

1. Data in motion, at rest; in applications, database security, DLP
2. Threat Management,
3. Network Security: perimeter security defense, routers, firewalls, tunneling,etc.
4. Endpoint Management: security patching, security compliance management.
5. Security Intelligence: SIEM, incident response, digital forensics.
6. Security models and architectures.

Compliance & Operations

1.Industry Compliance: SOX, HIPAA, NERC-CIP, GLBA.

2.Operational Resilience, Business Recovery, Legal Aspects

3.Industry Solutions – non traditional endpoints, embedded systems, implications of industry innovations: Smart Grid, Smart Buildings, Connected Home.

4.Security Operational Centers- SOC-NOC integration.

5.Educational Resources

Cyber Security Operations Center for Educational Purposes

Provide students with hands-on approach to learning Cyber Security and to experience real world challenges.

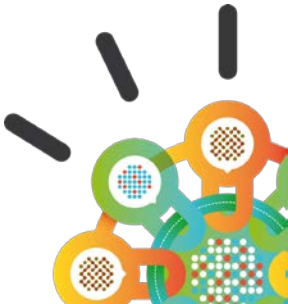
Specific tasks may include:

- Monitor university or other networks (real and/or simulated)
- Students perform assessment of security events, learning approaches on response to security breaches, and forensics, mitigation techniques
- Students can build dashboards, build reports, and learn the tools to be most effective
- Students learn to anticipate future threats based on behavioral analysis using real-time and historical data

This hands-on lab could be equipped with monitors, network intrusion detection devices, application scanning software, security intelligence software, among others.

Agenda

1. Cybersecurity is Imperative to Industry
2. Findings from a Cybersecurity Survey
3. IBM Initiatives to Support Cybersecurity Education
4. Concluding Remarks



Concluding Remarks –

- Become an active participants of the ecosystem to build security skills by contributing with your expertise
- Ensure cybersecurity education is pervasive across all disciplines – business, public policy, engineering, computer science, etc.
- Build capabilities to *the new perimeter of systems and solutions* – beyond the network
- Approach security with big data & analytics – *behavior analysis*
- Promote “hands-on” approaches that would allow students to move beyond classroom exercises


IBM