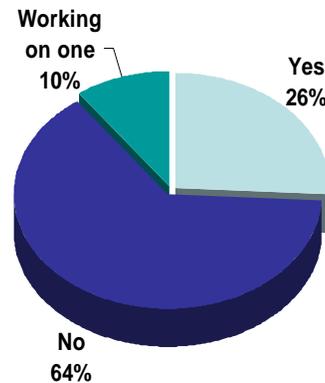


Profile of Participants in Survey

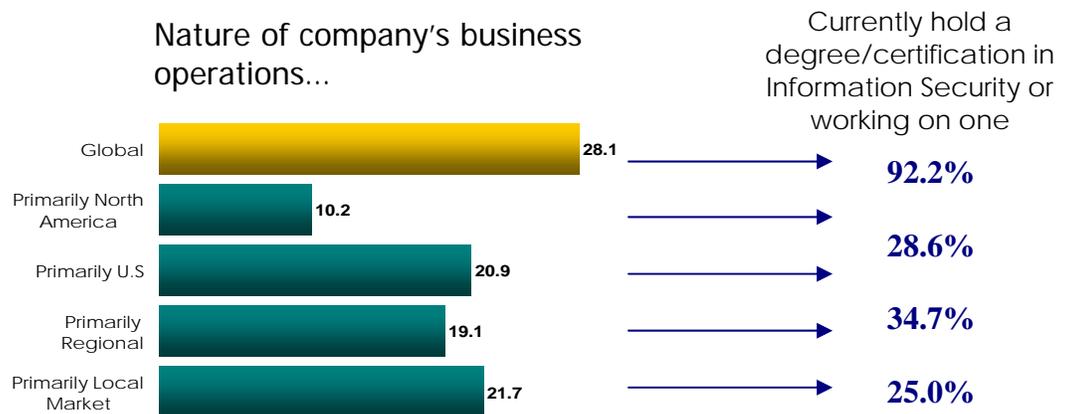
- Among those Information Security professionals participating in the study, 36% indicated that they currently hold a degree/certificate in information security or are currently working on one.
- Perhaps more indicative of the evolving nature of the Information Security profession and opportunity for defined practices and standards is the two-thirds or 64% who work in Information Security position but currently cite that they do not have a degree or certificate.
- The nature of their business would appear to be a strong indicator of their current "stage" of information security development. Ninety-two percent of respondents from companies with global operations cited having a degree and/or certification in Information Security as compared to less than 35% of those with primarily US operations and an average of 27% of those with regional or local focus.

36% currently hold a degree/certificate in information security or are currently working on one

Do you hold a degree/certification in Information Security?



Nature of company's business operations...



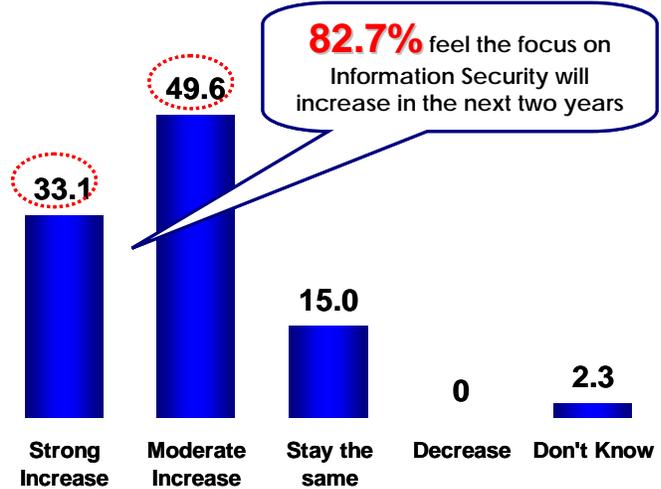
92% of respondents from companies with global operations cited having a degree and/or certification in Information Security

Future Outlook regarding the Focus on Information Security

- Eighty-three percent of respondents anticipate seeing a moderate to strong increase in the “focus” on Information Security in their company in the next 2 years. This figure is comparable to the results of a recent study conducted by Accenture/IDC released in December 2006 which found that 90% of executives stated that the security of data was a top priority for the new year.
- The graph below reflects the responses of respondents segmented by their respective industry. Those industries with above average anticipated focus are Government, Information, and Finance.

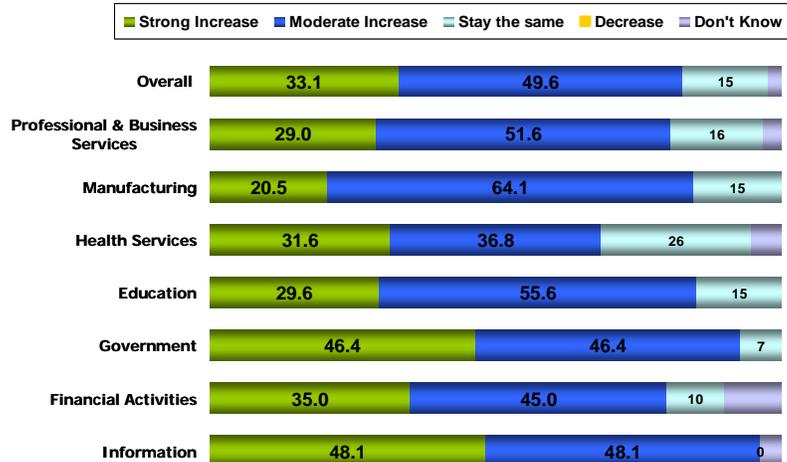
83% anticipate the focus on Information Security to increase in the next two years

In the next 2 years, how would you assess the focus on “Information Security” for your company?



33%
 feel their company's focus on Information Security will strongly increase in the next two years

In the next 2 years, how would you assess the focus on “Information Security” for your company?



Current Allocation of Budget to Information Security

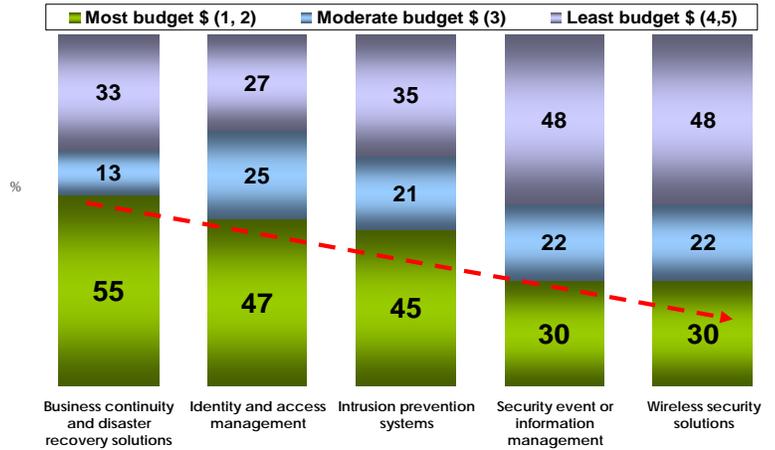
Under the heading of “Information Security,” technology solutions currently receiving the largest **budget allocations** are: (See Glossary for definitions)

1. **Business continuity & disaster recovery solutions**
2. **Identity and access systems**
3. **Intrusion prevention systems**

A recent Accenture/IDC study released in late December 2006 confirms that despite security ranking as a top priority among IT executives surveyed as part of the study, only about 10% of the budget is dedicated to security products and services with the majority being spent on operational or process aspects such as network, data center, operations and desktop.

Viewing the prioritization of budget allocations by industry segment, the top 2 areas of Information Security that are budgeted for by industry, results reflect common areas however prioritization varies depending on industry focus. For example among companies in the Financial and Health Services industries, “identify and access management” is priority while “intrusion prevention” is top of mind among those in manufacturing and government entities.

Thinking about Information Security within your company, please rank the following technology solutions in order of amount of budget allocated to this: Rank 1 to 5 where 1=Most budget \$

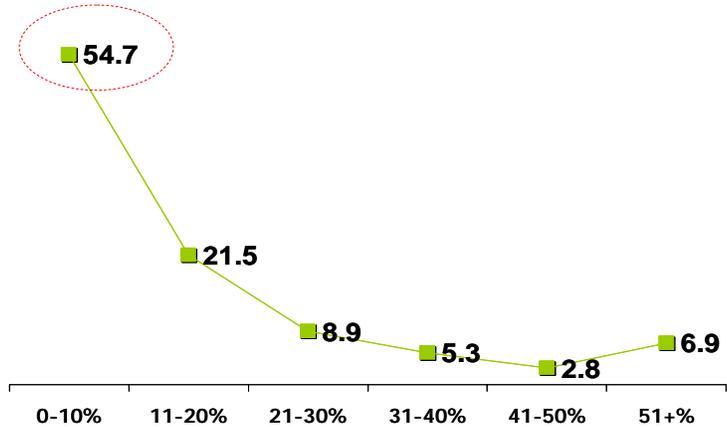


Industry	#1 budget allocation focus	#2 budget allocation focus
Education	Business Continuity & Disaster Recovery	Identity & Access Management
Financial	Identity & Access Management	Intrusion Prevention Systems
Healthcare	Identify & Access Management	Business Continuity & Disaster Recovery
Manufacturing	Intrusion Prevention Systems	Business Continuity & Disaster Recovery
Professional Business Svcs	Business Continuity & Disaster Recovery	Intrusion Prevention Systems
Government	Intrusion Prevention Systems	Business Continuity & Disaster Recovery
Information	Business Continuity & Disaster Recovery	Intrusion Prevention Systems

Low Spending on Personnel and Training

- Approximately 55% of employers surveyed state that they currently spend less than 10% of the information security budget on **personnel and training** while 76% spend less than 20% on personnel and training.
- Viewed by industry (graph below), those industries spending a higher than average percent of their information security budget on personnel and training are Information, Professional Business Services and Finance.

What percentage of your information security budget is currently spent on personnel and training?

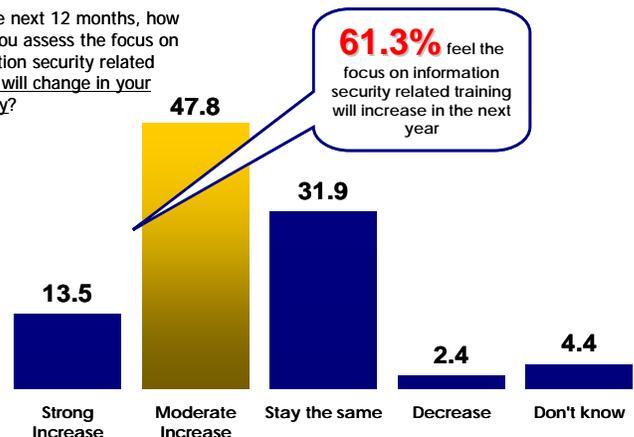


Industry	Average % of Information Security Budget spent on Personnel & Training	% indicating their "focus" on Information Security will <u>strongly increase</u>
AVERAGE	16.2%	33.1%
Education	16.7%	29.6%
Financial	18.5%	35.0%
Health Services	17.7%	31.6%
Manufacturing	11.1%	20.5%
Professional Business Svcs	18.7%	29.0%
Government	11.9%	46.4%
Information	20.3%	48.1%

Anticipated Growth regarding Future Allocations to Personnel & Training

- When asked about future plans for spending on personnel and training, ("over the next 12 months") two-thirds or 62% anticipate the focus on information security related training will increase; 48% anticipating a moderate increase with an additional 14% anticipating a strong increase.

Over the next 12 months, how would you assess the focus on information security related training will change in your company?

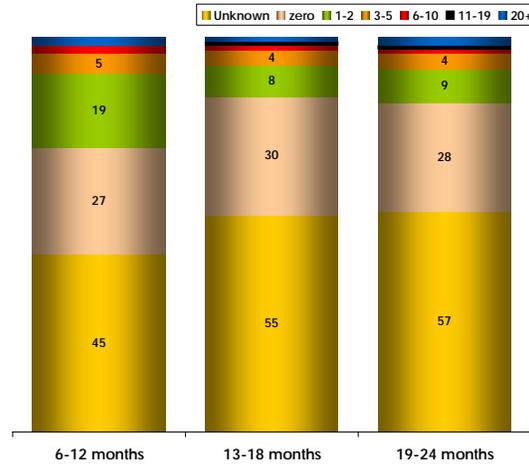


Anticipated Hiring of Information Security Personnel

- When asked about future “hires” of information technology/information security personnel within their company, the long-term needs are unknown, even among the profession. Among those responding to the survey, 20% anticipate hiring 1 or 2 new hires within the next 12 months, while 10% anticipated hiring 3 or more.
- When questioned about years 2008 and 2009, 85% indicated “unknown” or “zero” hires.



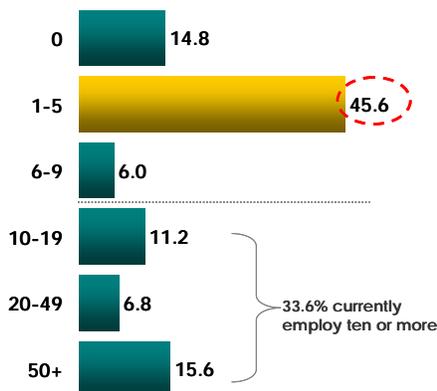
Approximately, how many information technology and/or information security professional “hires” is your company planning in the next... (Indicate the number for each time period)?



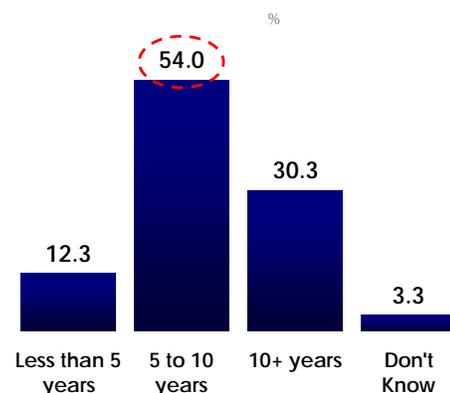
Currently Employed Security Personnel

- The current employment profile of Information Security personnel among employers is polarized with 46% of employers **currently employing** less than 5 information security professionals while 34% cite having more than 10.
- The Information Security industry as a career path would also appear to be polarized in terms of experience among current professionals. This could be attributed to the rapid evolution of careers within this profession. Over half of those information security personnel surveyed (54%) say that their dedicated information security personnel currently have between 5 and 10 years experience while approximately one-third say 10 or more years.

How many IT and/or information security professionals **do you currently employ?**



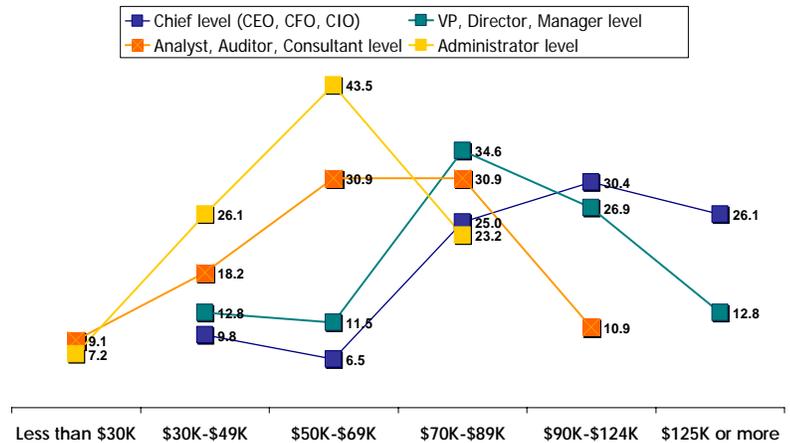
On average, how many **years of experience** do your information security workers have in the industry?



Salary Requirements for Information Security Professional Positions

- The graph to the right reflects perceptions of “average salaries” of Information Security positions, as provided by survey participants.
- For the purposes of this study, due to multiple titles, four classifications of positions were established and the average salaries associated with these positions were calculated as follows:

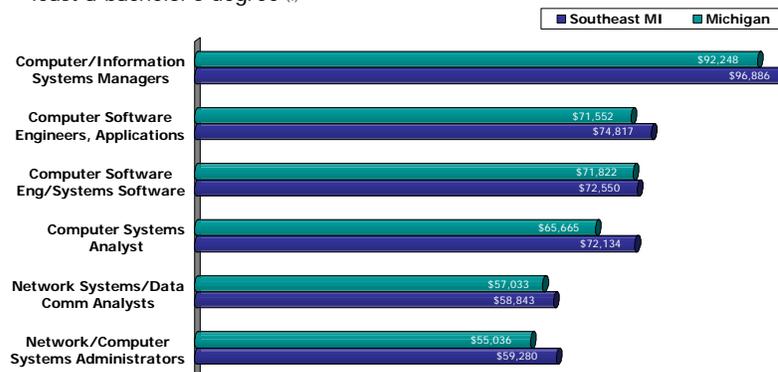
What are the average salaries of your information security professional positions?



- Chief Level (CEO, CFO, CIO) \$ 125,000
- VP, Director, Manager \$ 102,000
- Analyst, Auditor, Consultant \$ 65,000
- Administrator Level \$ 57,000

- For comparative purposes, the graph below reflects data reported by the Michigan Department of Labor & Economic Growth in their Career Outlook through 2012 publication.
- A comparison of the data provided by respondents in the survey would indicate salary expectations that are in-line with projections by the Michigan Department of Labor.

Annual Salary Comparison of high-growth occupations requiring at least a bachelor's degree ⁽¹⁾



Source: Michigan Department of Labor & Economic Growth, Bureau of Labor Market Information & Strategic Initiatives, Michigan Career Outlook Through 2012, 11/05.

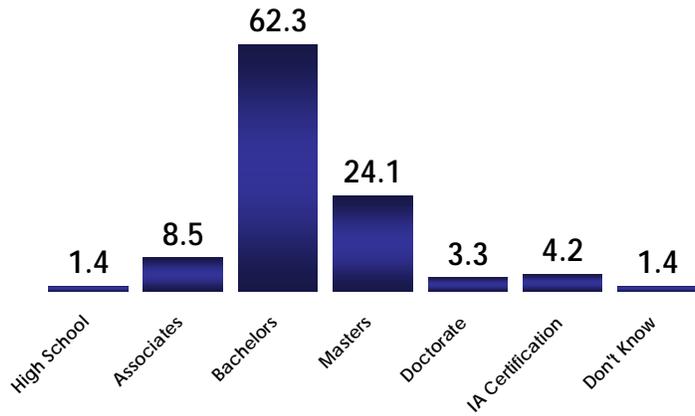
(1) Calculation of Annual Salary based on hourly wage cited or 2,080 annual hours

Snapshot of Requirements - Today and Future

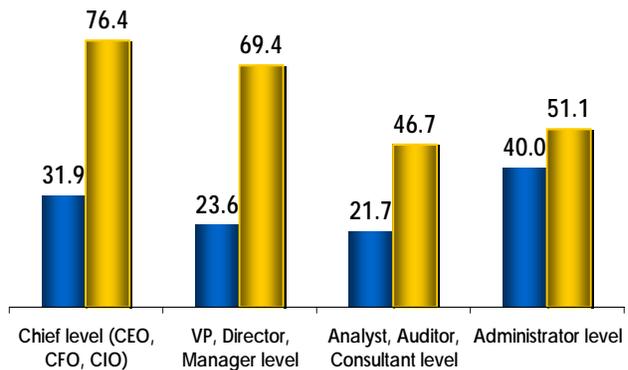
- Regardless of employment positions, 62% of employers surveyed, state that the highest level of education of their current information security professionals is a “Bachelors” degree.
- At least 50% of those responding to the survey indicate that they require any information security position to have a post-secondary degree at a minimum. This averages from 50% citing for information security administration positions to 80% indicating for IS Executive positions (i.e., CIO, CFO, CSO).



What is the average **highest level of education** of your current information security professionals?



■ Certification currently required ■ Degree currently required



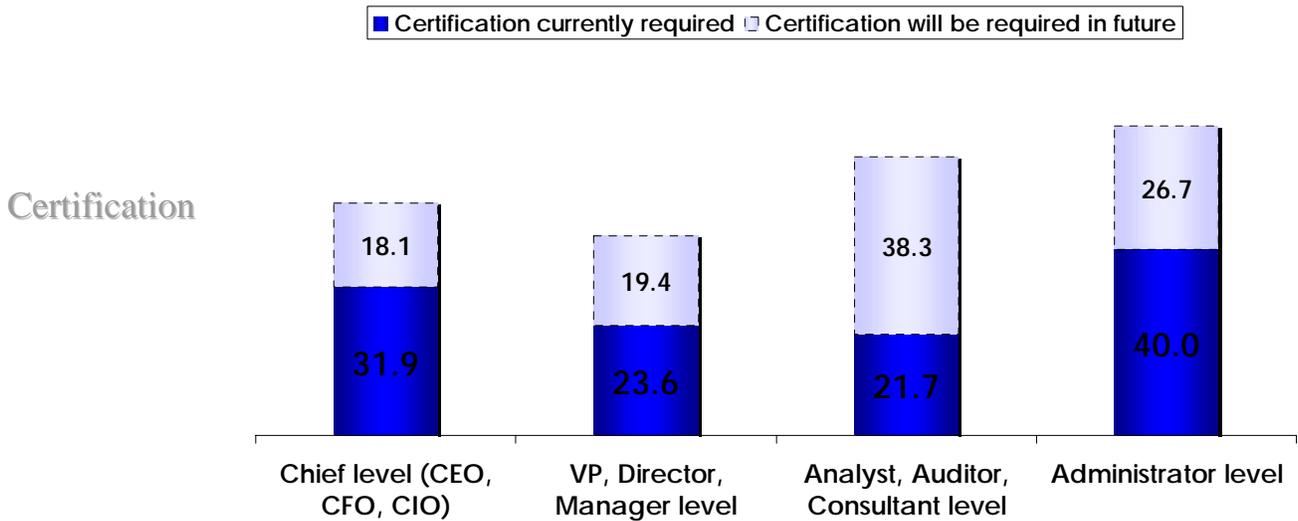
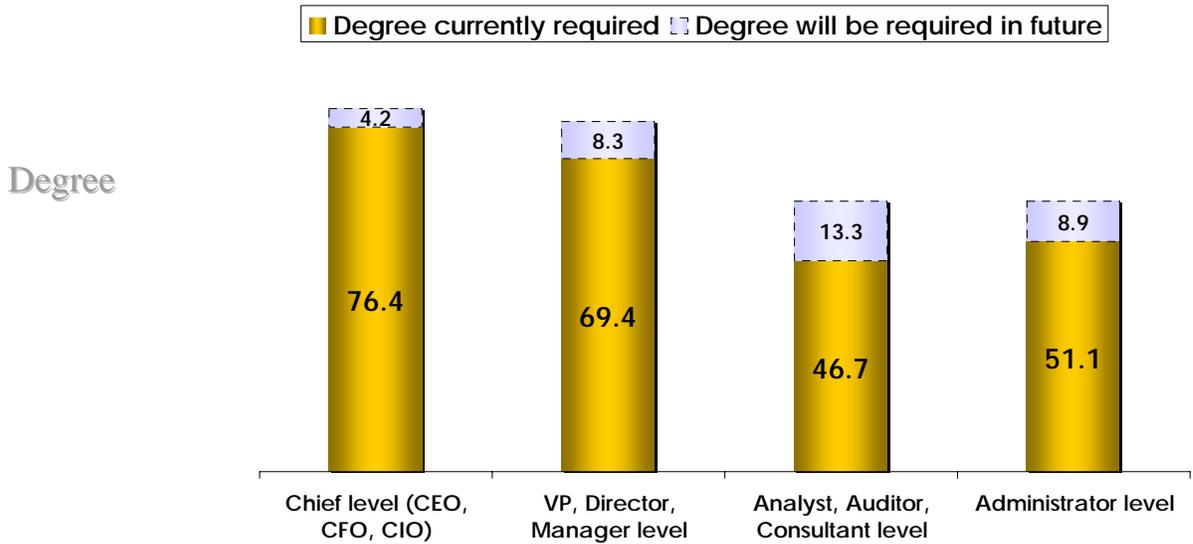
62%

Of employers surveyed, state that the highest level of education of their current information security professionals is a “Bachelors” degree

Need for Degree and Certification in Information Security Professions

- While 50% of information security personnel cite that their employers do not currently require a degree for IS administrative positions, 67% state that they currently require or will require “certification” in these positions.
- At least 60% of respondents indicate that in the future, a minimum of “certification” will be required for even IS administration positions.

Are security specific degrees or certifications required for these positions within your organization?

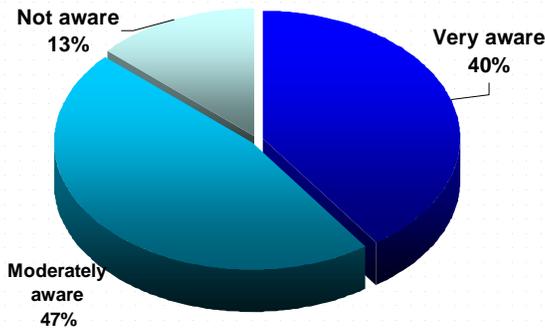


Awareness for Information Security degrees/certifications

- Approximately 87% say they are **very to moderately aware** of ways to get information security degrees and/or certifications. Approximately two-thirds (61%) claim to be aware of *some type* of specific IS certification and/or degree program.
- Forty-eight percent associate this program with “educational institutions” while 45% think of “training” institutions.
- Those respondents most aware of ways to get information security degrees and/or certifications are found in the Health Services, Finance and Manufacturing industries.

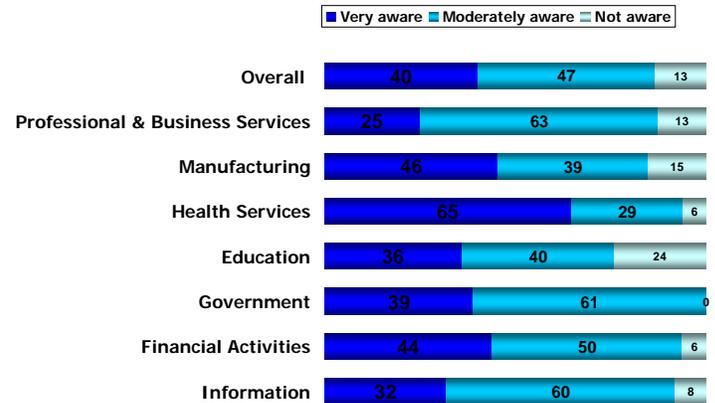
Awareness levels:

How aware are you of ways in which to get information security degrees/certifications?



87% are very to moderately aware of ways to get information security degrees/certifications

How aware are you of ways in which to get information security degrees/certifications?



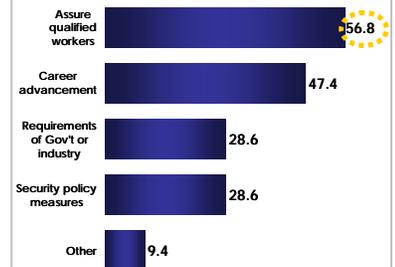
Perceptions Surrounding Information Security degrees/certifications

- When asked “What are the primary reasons for obtaining **security degrees and/or certifications?**”, the top two reasons are:
 - To assure qualified workers
 - Career advancement

To assure qualified workers	57%
Career advancement	47%
Requirements of Government or Industry	29%
Security policy measures	29%

Reasons to obtain:

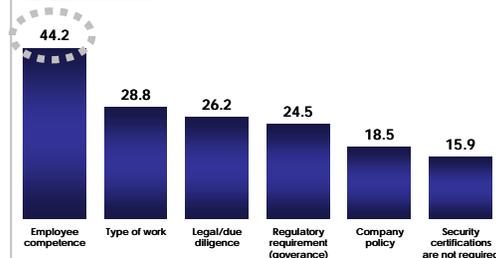
Why are security degrees/certifications currently required, or why would you obtain these? (multi-select)



- The **primary reasons** employers would “hire” an information security professional with a degree or certification would be:

- Employee competence
- Type of work
- Legal/due diligence
- Regulatory requirements

What are the **reason(s) you would hire** an information security **degreed/certified** professional? (multi-select)



70% feel Information Risk Management top new frontier for information security training

The Top 5 Training Frontiers

- In terms of the next **TOP 5 new frontiers** for “information security training and degree/certification” in the next 1-3 years:
 1. Information Risk Management
 2. Security Management practices
 3. Business continuity and disaster recovery planning
 4. Access control systems and methodology; and
 5. Auditing

What do you believe will be the **TOP 5 new frontiers for information security training and degree/certification in the next 1-3 years?** (Base: Top 5 by overall mention)



The Top 5 Training Frontiers – Focusing by Industry

- While the Top 5 could be considered consistent among all employers, a deeper view by industry reveals some variation in prioritization. While those in Professional Services, Health Services and Financial top their list with “Security Management Practices”, information security professionals in Manufacturing, Education and Information would put “Information Risk Management” at the top of their list.
- Greater insight into the “definition” of these priorities could reveal specific training/certification initiatives that could be targeted to specific industry segments.

	1	2	3	4	5
Professional & Business Services	Security management practices (71%)	Business continuity & disaster recovery planning (64%)	Information Risk Management (61%)	Access control systems & methodology (46%)	Application & systems development security (32%)
Manufacturing	Information Risk Management (70%)	Business continuity & disaster recovery planning (64%)	Security management practices (61%)	Auditing (46%)	Access control systems & methodology (39%)
Health Services	Security management practices (80%)	Information Risk Management (73%)	Business continuity & disaster recovery planning (73%)	Auditing (53%)	Access control systems & methodology (40%)
Education	Information Risk Management (76%)	Security management practices (62%)	Access control systems & methodology (62%)	Business continuity & disaster recovery planning (57%)	Auditing (48%)
Government	Business continuity & disaster recovery planning (63%)	Auditing (63%)	Information Risk Management (56%)	Security management practices (56%)	Forensics (38%)
Financial	Security management practices (86%)	Information Risk Management (57%)	Access control systems & methodology (43%)	Business continuity & disaster recovery planning (36%)	Forensics (36%)
Information	Information Risk Management (74%)	Business continuity & disaster recovery planning (68%)	Security management practices (58%)	Access control systems & methodology (53%)	Application & systems development security (53%)

Employer Information Security Survey



- **Benchmark and measure the degree of assessed importance and prioritization of Information Security initiatives among Southeast Michigan companies;**
 - Information sources impacting their perceptions
 - Current and emerging requirements of their industry and/or government regulations
- **Benchmark their current assessed stage of Information Security (i.e., early/minimal, mid-range, mature/maximum) relative to their industry**
- **Identify and define current human resources, budget allocations and initiatives in place or being planned for Information Security purposes among SE Michigan business;**
 - Outsourcing, Partnerships
- **Prioritize the needs of businesses (by industry sector and size) who define Information Security as a key strategic initiative for their company;**
- **Identify and define current employment positions in Information Security and/or current outsourcing;**
 - Benchmark anticipated employment projections
 - Identify needs in training, skills development and technologies to meet future goals;
- **Profile company for segment analysis**
 - Industry sector
 - Size of Business/Organization
 - Markets Served (regional, national, global)

Methodology used in data collection

Research Approach:

- **Targeted respondents:** Personnel identified as “responsible for company and business Information Security issues” (i.e., Chief Information Security Officer, CEO, CIO, CSO, Director of Security, Director/Manager, Network Administrator, Security Analyst, Security Auditor, Security Consultant/Manager)
- **Approach:** Due to the potential security and sensitivity of the questions being asked, a confidential response survey approach was recommended.
 - **Automation Alley members:** Contact via-email - **Pre-notification** to all Automation Alley members by Automation Alley of importance and value of survey and potential contact. Automation Alley contacts will be asked to forward the survey link to the person internally who is responsible for Security decisions.
 - **RSA Partner companies:** Contact via e-mail and/or paper questionnaire.
 - **SE Michigan Security Decision makers (outside AA membership):**
 - Personal contact and completes was accomplished via on-site questionnaire distribution at the 2006 SecureWorld Expo, on September 19th and 20th, 2006. Hard copy surveys were distributed to attendees to complete and return on-site at the Automation Alley booth.
 - Telephone contact via phone from business cards was provided at the Expo as well as Intellitrends lists. Phone surveying was implemented following the Expo to determine any requirements in specific industry categories.
- **Survey positioning:** The survey was positioned as sponsored by:
 - Automation Alley and Southeast Michigan Information Security RSA under a grant from the Department of Labor and Economic Growth (DLEG)
 - All responses were confidential and anonymous. Only aggregate results will be reported
 - For their participation, respondents will receive an “Overview Paper” on the topic to be mailed upon completion (also available via AA web-site)



intellitrends
A Market Vision and Strategy Company

Intellitrends LLC
8031 M-15, Suite 120
Clarkston, MI 48348

Automation Alley

Automation Alley drives the growth and image of Southeast Michigan's technology economy through a collaborative culture that focuses on workforce and business development initiatives.

Since its founding in 1999, Automation Alley has expanded to include more than 700 businesses, educational institutions and government entities, covering an eight county area and the City of Detroit. Automation Alley promotes regional prosperity through the Automation Alley International Business Center, which provides business attraction services and exporting assistance; the Automation Alley Technology Center, which brings together businesses, educators and government to help entrepreneurs accelerate technology commercialization; and the GLIMA Network, a state-wide association for individuals engaged with and involved in technology-oriented industries.

Keith Stone
Executive Vice President/COO
248-922-3344
kwstone@intellitrend.com
www.intellitrend.com

Founded in 1989, Clarkston, Michigan based, Intellitrends provides its clients with a broad range of market and consumer research capabilities, including telephone and online surveys, focus groups, executive research, and customer and employee satisfaction studies. The company's clientele includes DaimlerChrysler, Masco Corporation, Little Caesars Enterprises, Macomb County and many others. For more information, please visit www.intellitrend.com