intellitrends
A Market Vision and Strategy Company

Information Security and Southeast Michigan Business

A Market Opportunity and Needs Analysis of Southeast Michigan Businesses for Information Security Resources

January 25, 2007

Southeast Michigan Information Security Regional Skills Alliance (RSA)
Karen Thompson, Manager, Information Security (RSA)

Private & Confidential

The following is considered a private and confidential and no other person or organization may copy any part of the following for purposes of implementation, discussion or forwarding to another organization without the prior consent of Intellitrends, LLC.

Table of Contents

Background

Executive Summary

Study Overview

Key Findings

Appendix

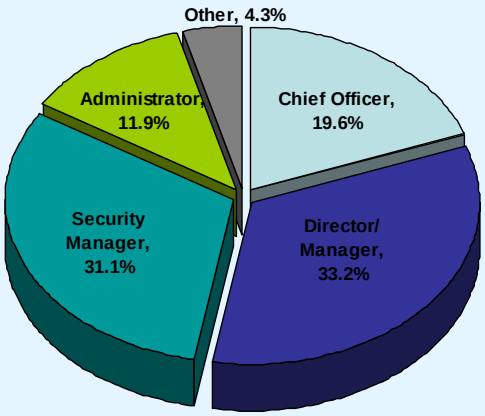
Background

The following study, implemented from September through December 2006, was a research initiative sponsored by Automation Alley and the Southeast Michigan Information Security Regional Skills Alliance (RSA) under a grant from the State of Michigan Department of Labor and Economic Growth. In alignment with the importance of the increasing and evolving needs of Southeast Michigan employers regarding Information Security career and skills, the RSA also recognizes the importance of having a skilled and training IA workforce. The goal for the research was to serve as a framework and enhance the development of a focused plan to meet the vision of the RSA: **By 2009,**

- Southeast Michigan Information Security RSA will be recognized as the model for how to create the best trained workforce in the United States.
- The RSA will have shared supporting research and data with employers for them to incorporate into their strategic and operational planning efforts and will have provided these employers access to the best trained workforce in the U.S.
- The RSA will provide K-20 timely and accurate information security career pathways and required training information network for information security occupations in Southeast Michigan.
- The RSA will be the recognized channel for employers and educators/trainers and employees seeking information on security career pathway ladders and required training for occupations in the healthcare and homeland security industries.

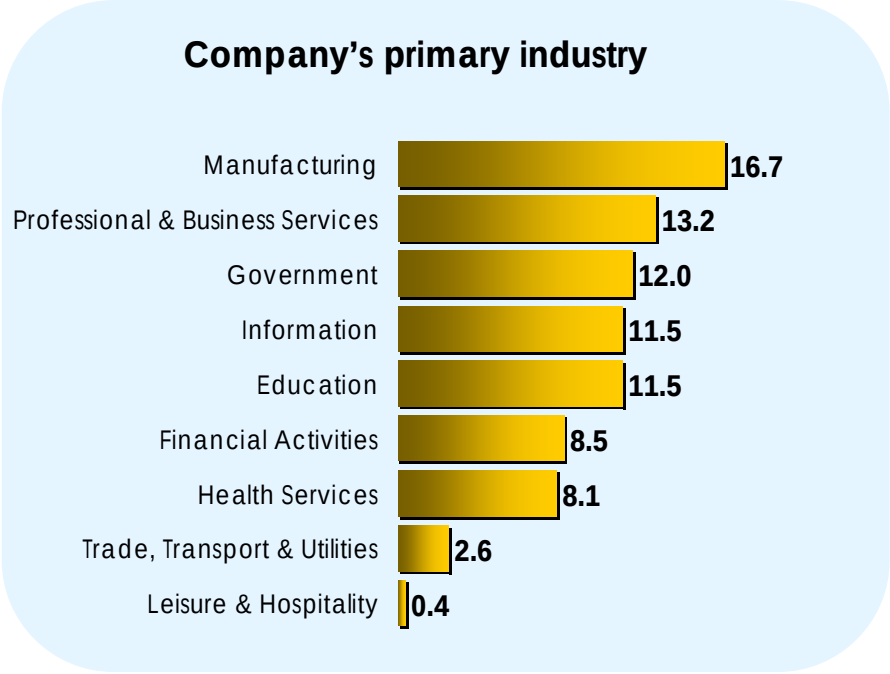
The research reflects the responses of 261 Information Security personnel in Southeast Michigan businesses (reflective of a +/-6.0% margin of error at 95% confidence interval.) Respondents to the survey were contacted via multiple avenues; Secure World Expo, held September 19th and 20th, phone contact, direct distribution at the Automation Alley Fall Networking event (Kettering University – October 26th, 2006) and web-based survey to Information Security personnel through Automation Alley member companies.

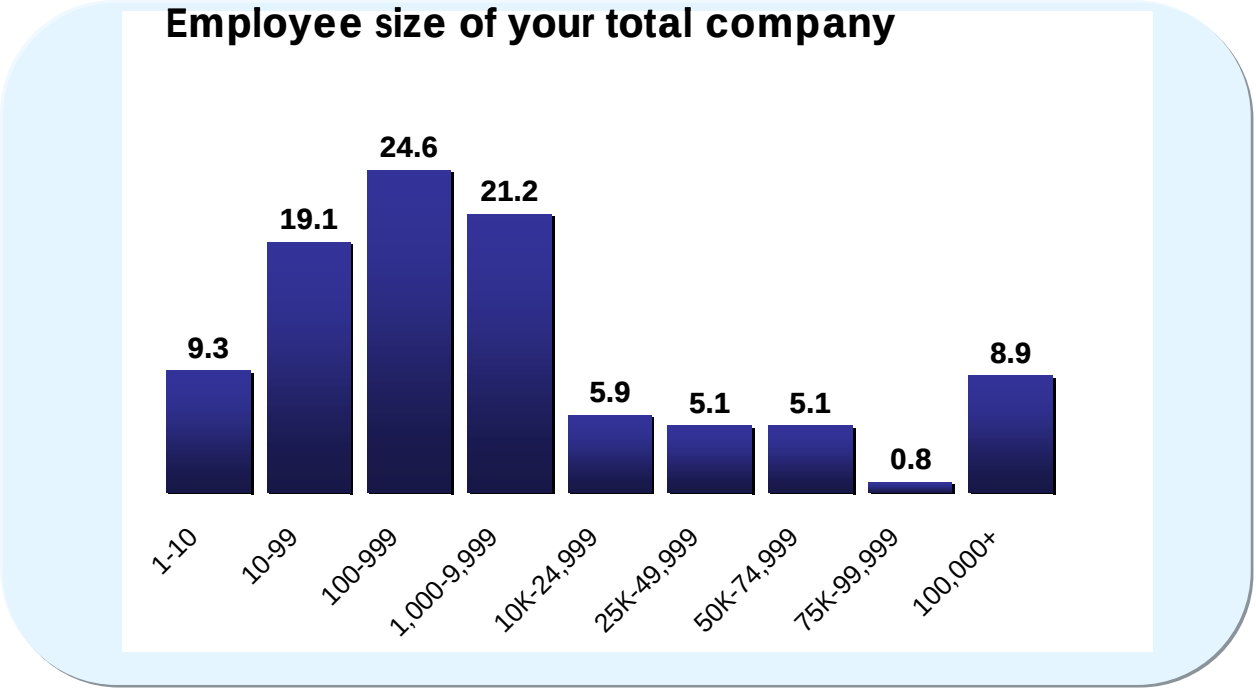
Profile of Study Participants



While no quotas were able to be established for specific industries or types of operations, the results reflect a strong cross-section of the Southeast Michigan business community both in terms of industry focus as well as size of company.

Approximately 28% of Information Security personnel worked for companies with up to 100 employees, 25% for companies with between 100 and 999 employees, and the balance 47% for companies with an employee base in excess of 1000.





Executive Summary

Trends in Information Security

Information security is defined as "the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption.[1] Sometimes referred to as information assurance the two terms are often used interchangeably but share the common goals of protecting the confidentiality, integrity and availability of information.

According to the U.S. Government's National Information Assurance Glossary, it is defined as:

> *Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*

The rapid evolution of technology has made today's businesses increasingly aware of and challenged by the critical need to have processes, controls and security in place to challenge the ever evolving, complex and unpredictable breaches of security. These breaches cannot only expose confidential information about employees, clients, their products and financials but also subject companies to operational, financial, and market risk. Perhaps one of the most highly publicized examples of a drastic and unimagined breach of information security occurred in 2005, when a missing laptop from the U.S. Department of Veterans Affairs put more than 20 million veterans and their personal information at risk. Since that incident, the issue of information security has become highly charged among the public and in turn placed immediate demands on action by businesses.

A recent forum of Information Security professionals conducted by SANS Institute (SysAdmin, Audit, Network, Security) in 2006, identified and re-verified what they coin as "The Ten Most Important Security Trends of the Coming Year." Topping the list were the use and control of "mobile devices" (i.e., Laptops, PDAs, Smart phone). These devices continue to proliferate as tools of efficiency but also represent higher risk as customer/patient/product data is installed and/or accessible with this new equipment. The third most important was the impact of government legislation regarding the protection of customer information. Increased regulations imply greater risk of penalties on organizations that lose sensitive personal information. Fourth and fifth were "targeted attacks" in the form of cyber attacks of other global areas against US government systems as well as on commercial organizations that hold valuable customer information. Grouped with targeted attacks are "cell phone worms" and "voice over IP" systems which can infect instantaneously and multiple exponentially through wireless networks. Cell phones with full operating systems and access to software development environments are anticipated to be targets. Rounding out the top ten list was spyware, cited as a "huge and growing issue" as were "0-day vulnerabilities" and "rootkits" which can change an operating system to hide an attacker's presence and make it impossible to uninstall the malware.

Trends among Southeast Michigan Businesses

The results of the Southeast Michigan 2006 Employer Information Security Survey study, completed in December 2006 among 261 Information Security professionals **revealed a strong awareness for and commitment to the issues of addressing information security**, however a gap between the focus and actual realization still exists. Eighty-three percent of those surveyed agreed the focus on Information Security at their company will increase in 2007 with one-third citing a "strong increase," however this study also found that over half are spending less than 10% of their budget on information security initiatives and three-quarters currently allocate less than 20% to personnel and training. This important finding is in-line with national findings.

A study recently released by Accenture/IDC in December 2006 in which IT executives were surveyed also found that **more than 90% agreed that information security was a top priority** for the coming year. However, in stark comparison less than 10% of their IT budgets are currently being spent on products and services to secure data. (2)

Among Southeast Michigan businesses, solutions currently receiving priority in budget allocations could be classified under the heading of immediate protection; "business continuity and disaster recovery solutions," identify and access management" and "intrusion prevention systems."

However, the opportunity for action is beginning to expand rapidly. When asked about the next 12 months, two-thirds of Southeast Michigan companies surveyed cited commitments to increased spending on information security training with the most aggressive being in those industries of Finance, Information and Professional Business Services. Currently, the information security industry would appear to be polarized in terms of staffing as well as education requirements. Among SE Michigan businesses, almost half (46%) currently employ less than 5 dedicated information security professionals while 22% indicate having more than 20. In terms of experience, over half (54%) indicate their information security personnel have between 5 and 10 years experience as compared to one-third indicating more than 10 years.

As a career path nationally, the field of Information Security is projected to grow faster than average job growth. According to the Bureau of Labor Statistics, both nationally and Michigan, careers in computer systems including management, engineering, and support will top the list as the fastest growing occupations through 2012. Global initiatives for standard practices and principles as well as increasing convergence led by U.S. global companies will set the stage for strong growth. In the next 12 months, 30% of Southeast Michigan business anticipates new hires. According to the Southeast Michigan Department of Labor, job growth through 2012 will average between 27% for Computer and Information Systems Managers and up to 50% for Network Systems and Data Communications Analysts.

In addition to computer related skills, the field now embraces unique and defined career paths such as Information Systems Auditing, Business Continuity Planning and Digital Forensics Science. In response to increasing specialization, minimum educational expectations for information security positions are continuing to increase. Half of Southeast Michigan business surveyed indicated that *any* information security position now has the expectations of a security related degree (level non-specified). For executive management positions (CIO, CFO, CSO), over 80% of those surveyed indicated this was a base requirement. While one in two indicated that a degree was not required for information security positions, over two—thirds indicated that some type of "certification" was and will be a minimum requirement. These increased education requirements are directly related to assuring "qualified workers" and for "career advancement."

As reflected through this study, "certification" as an educational initiative is taking hold yet is still primarily among businesses with a global presence. When respondents to this survey were asked if they held a degree or certification in Information Security, 92% of those with global operations indicated "yes" as compared to less than 35% with primarily US operations and 27% of those with primarily regional or local market businesses.

The Information Security profession to this point has been defined through a reactive environment. In the mid 1990's formalized guidelines and practices were initially established to address the government initiative "Computers at Risk" and were formalized under the acronym "GASSP" Generally Accepted *System* Security Principles. Under an evolving and reactive environment, the organization and its guidelines became fragmented and disparate.

In 2004, principles and practices were outlined in a publication, based on:

(1) Rapid globalization of business and government
(2) Growth and proliferation of the Internet as a tool for business and the public
(3) Heightened awareness and demand for security in the public
(4) New initiatives by the U.S. government (i.e., Homeland Security, Partnership for Critical Infrastructure Protection)
(5) The need for protection and security while minimizing the regulatory affect on free markets
(6) Creation of industry standards for technology protection (ISO 17799, now ISO 27002)

It is advocated by GAISP (changed to Generally Accepted *Information* Security Principles) that the Information Security profession must follow the examples of other industries who have successfully adopted and adhere to nationally and internationally recognized practices and principles such as GAAP for Certified Public Accountants. In addition, the need to integrate formalized guidelines into the technology management function is key. (3) This "convergence" or integration of traditional and information security is increasingly being adopted by U.S. companies with global operations not only as a need to protect but also as a value-added competitive advantage. A 2005 study by Booz Allen Hamilton(4) with CSOs (Chief Security Officers), CISOs (Chief Information Security Officers) pointed to several factors propelling this convergence:

- Adherence to risk assessment requirements under Sarbanes-Oxley
- Focus on security at a higher strategic operational level (integral to corporate risk)
- Company need to protect "intangible" assets (i.e., knowledge, technology, know-how, skill-sets)
- Use of technology in traditional security functions (i.e., access passes)

From the results of the study and in light of initiatives globally, it is clear that the issue of Information Security and its professions is ready for aggressive initiatives. While 87% of Southeast Michigan businesses area "moderately" to "very aware" of ways to get information security degrees and/or certifications, only 60% to date are aware of a specific program or degree. While half associate this with an educational institution, the balance perceives it available through training institutions.

What's on their mind?

For Southeast Michigan business, the next Top 5 new frontiers for information security training and degree/certification through 2010 are defined as:

1. **Information Risk Management**
2. **Security Management Practices**
3. **Business Continuity and Disaster Recovery Planning**
4. **Access Control Systems and Methodology**
5. **Auditing**

(1) www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542
(2) "Security grabs attention, but not always dollars", January 2, 2007, John Moore.
(3) Generally Accepted Information Security Principles (GAISP), ISSA 2004
(4) Convergence of Enterprise Security Organizations, November 8, 2005, Booz Allen Hamilton.

Study Overview

A. Goals

In support of goals and objectives of the RSA, the specific goals of the research were to:

- **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 gov't 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)

B. Methodology used in data collection

The questionnaire tool to be used was developed by the RSA and is considered proprietary to this study.

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:

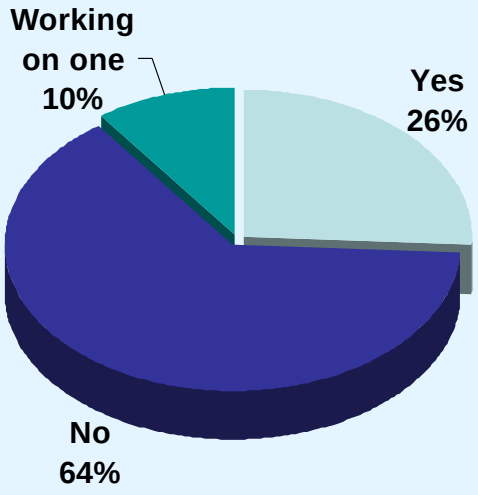
- Automation Alley and Southeast Michigan Information Security RSA under a grant from the Department of Labor and Economic Growth (DLEG)
- All responses were confidential and anonymous. Only aggregate results will be reported
- For their participation, respondents will receive an "Overview Paper" on the topic to be mailed upon completion (also available via AA web-site)

Key Findings

Profile of Participants in Survey

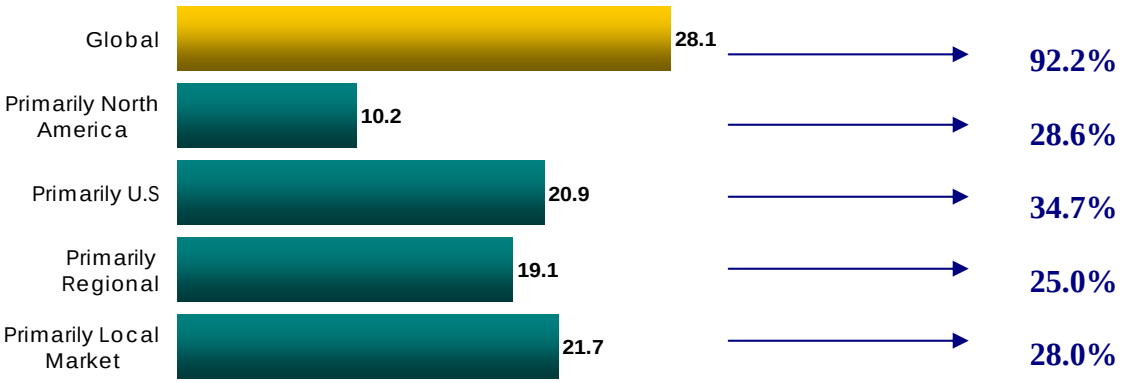
- Among those Information Security professionals participating in the study, 36% indicated that they currently hold a degree/certificate in information security or are currently working on one.
- Perhaps more indicative of the evolving nature of the Information Security profession and opportunity for 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 Infomration 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.

Do you hold a degree/certification in Information Security?



Nature of company's business operations...

Currently hold a degree/certification in Information Security or working on one

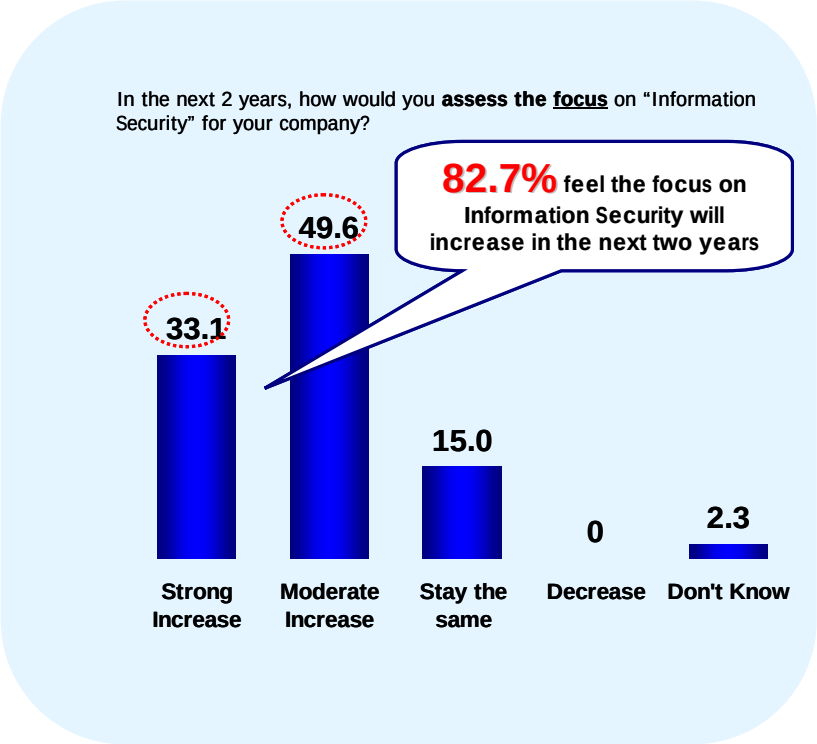


intellitrends
A Market Vision and Strategy Company

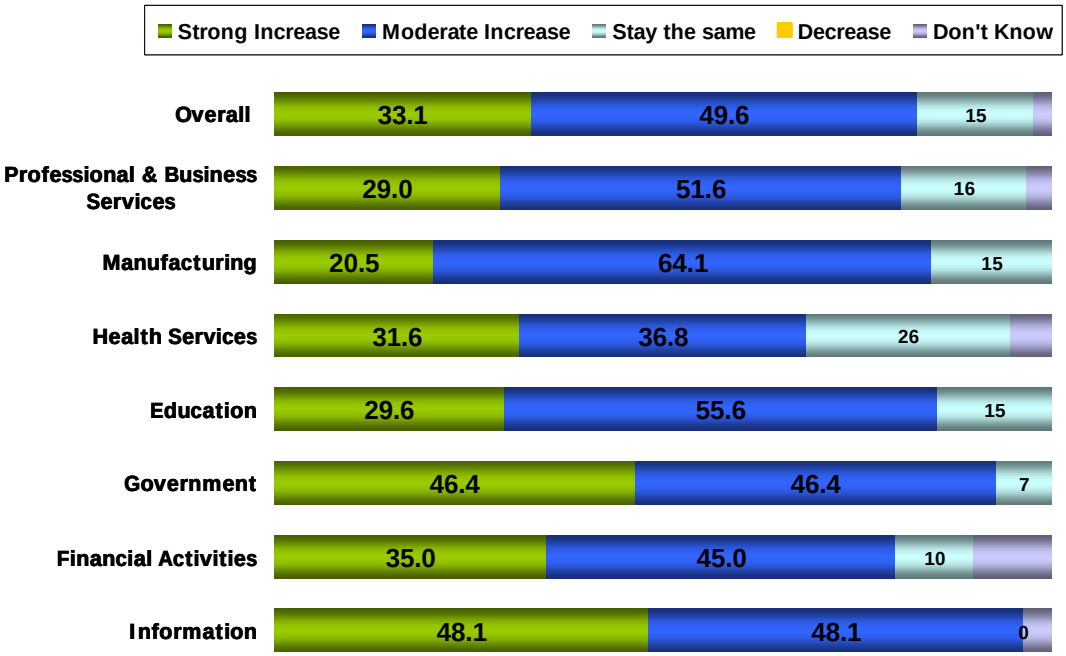
Future Outlook regarding the Focus on Information Security

- 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.



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



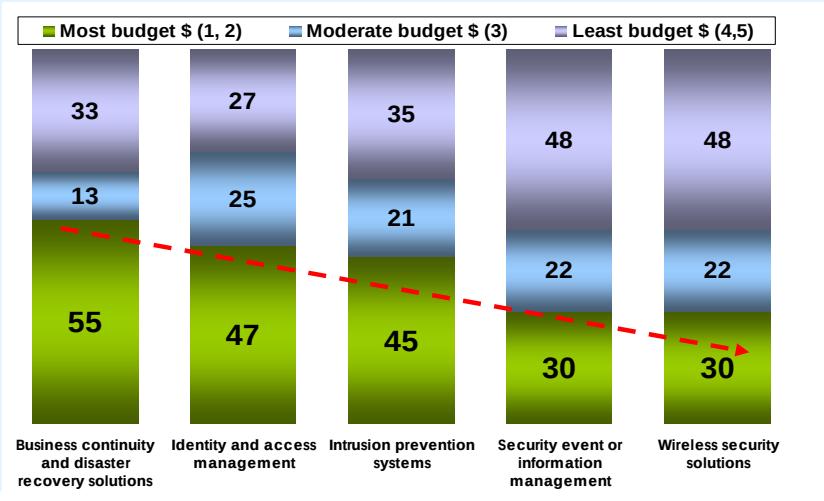
Current Allocation of Budget to Information Security

- 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 management**
  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.

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 $

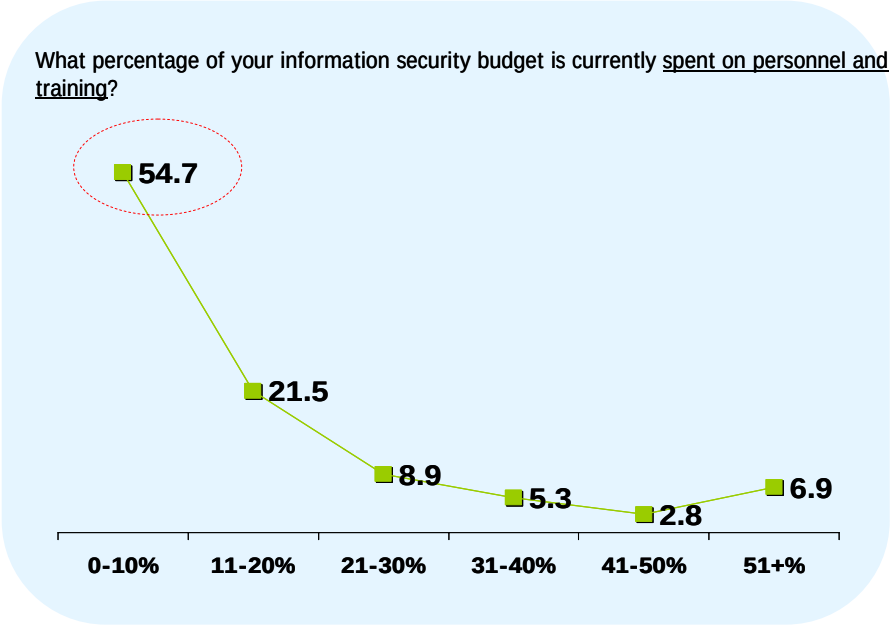


- Viewing the prioritization of budget allocations by industry segment, the top 2 areas of Information Security that are budgeted for by industry, results reflect common areas however prioritization varies depending on industry focus. For example among companies in the Financial and Health Services industries,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

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 Srvcs	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.



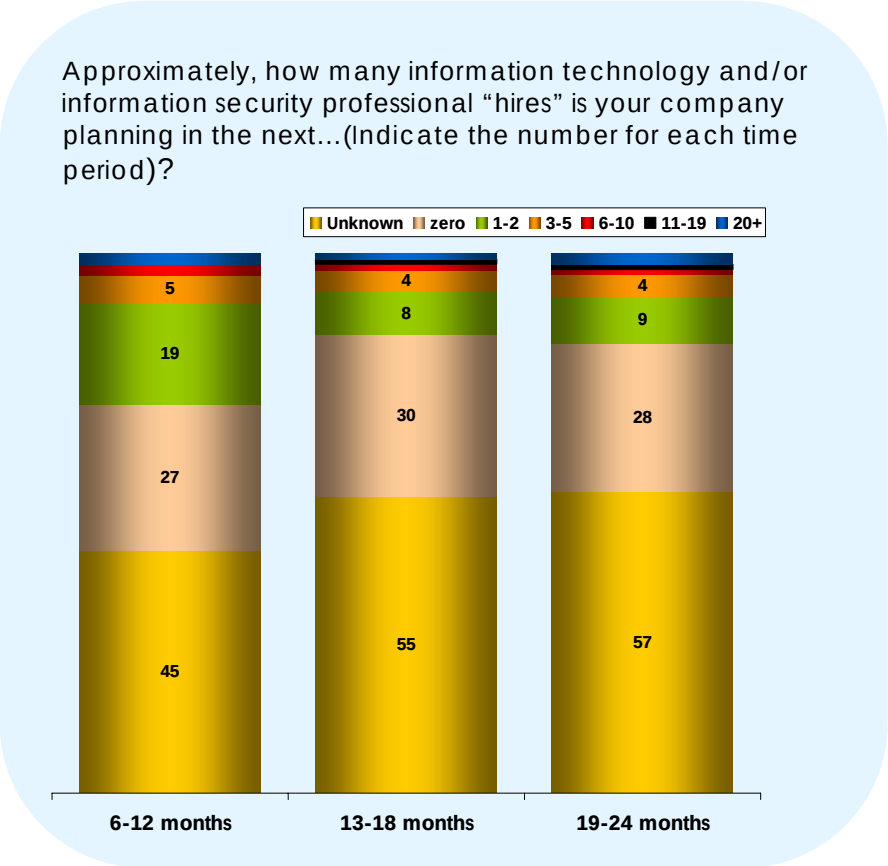
Industry	Average % of Information Security Budget spent on Personnel & Training	% indicating their "focus" on Information Security will strongly increase
AVERAGE	**16.2%**	**33.1%**
Education	16.7%	29.6%
Financial	18.5%	35.0%
Health Services	17.7%	31.6%
Manufacturing	11.1%	20.5%
Professional Business Srvcs	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.

Anticipated Hiring of Information Security Personnel

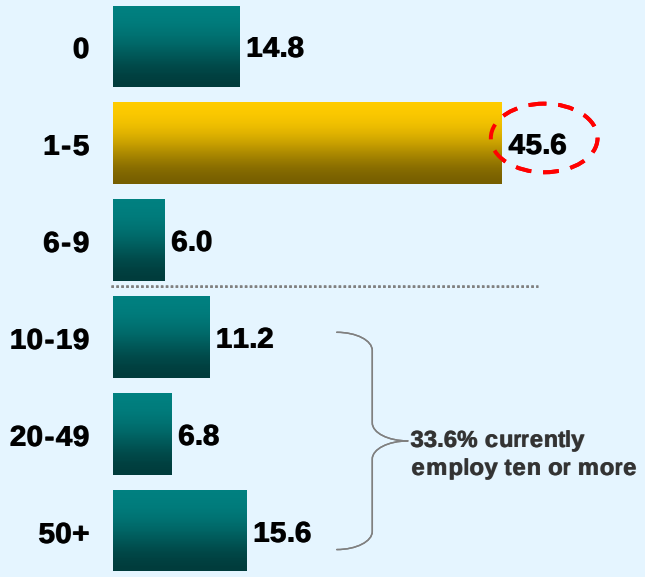
- When asked about future **"hires"** of information technology/information security personnel within their company, the long-term needs are unknown, even among the profession. Among those responding to the survey, 20% anticipate hiring 1 or 2 new hires within the next 12 months, while 10% anticipated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



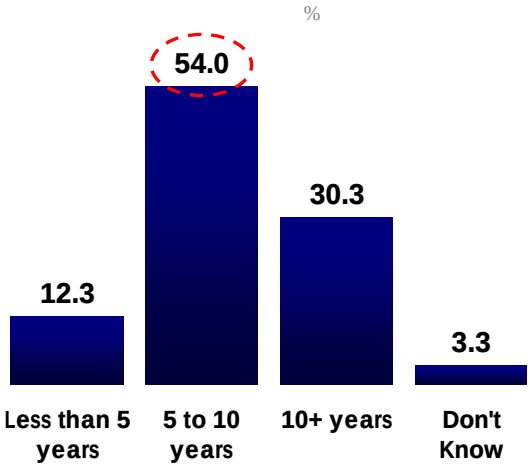
Currently Employed Security Personnel

- 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?

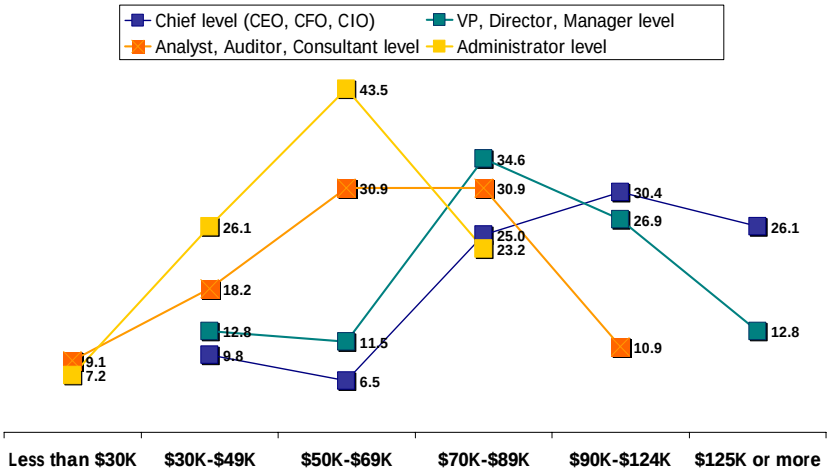


Salary Requirements for Information Security Professional positions

- 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?



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

- For comparative purposes, the graph to the right reflects data reported by the Michigan Department of Labor & Economic Growth in their Career Outlook through 2012 publication.

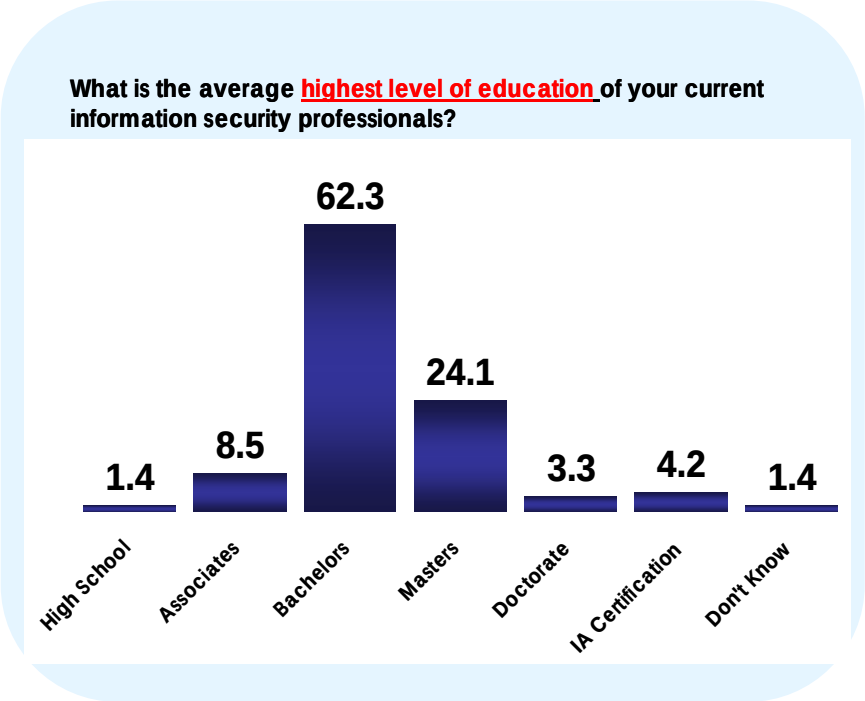
- A comparison of the data provided by respondents in the survey would indicate salary expectations that are in-line with projections by the Michigan Department of Labor.

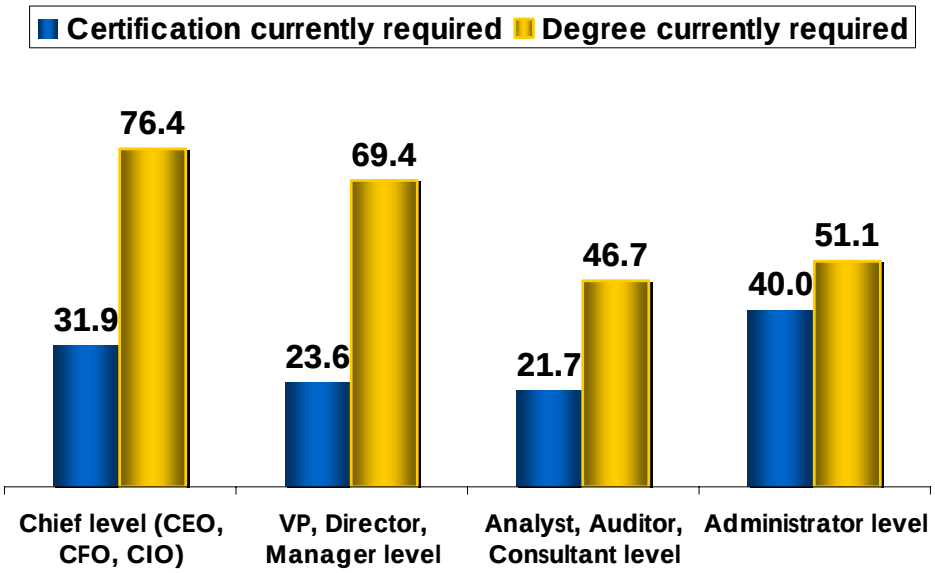
Annual Salary Comparison of high-growth occupations requiring at least a bachelor's degree (1)

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).

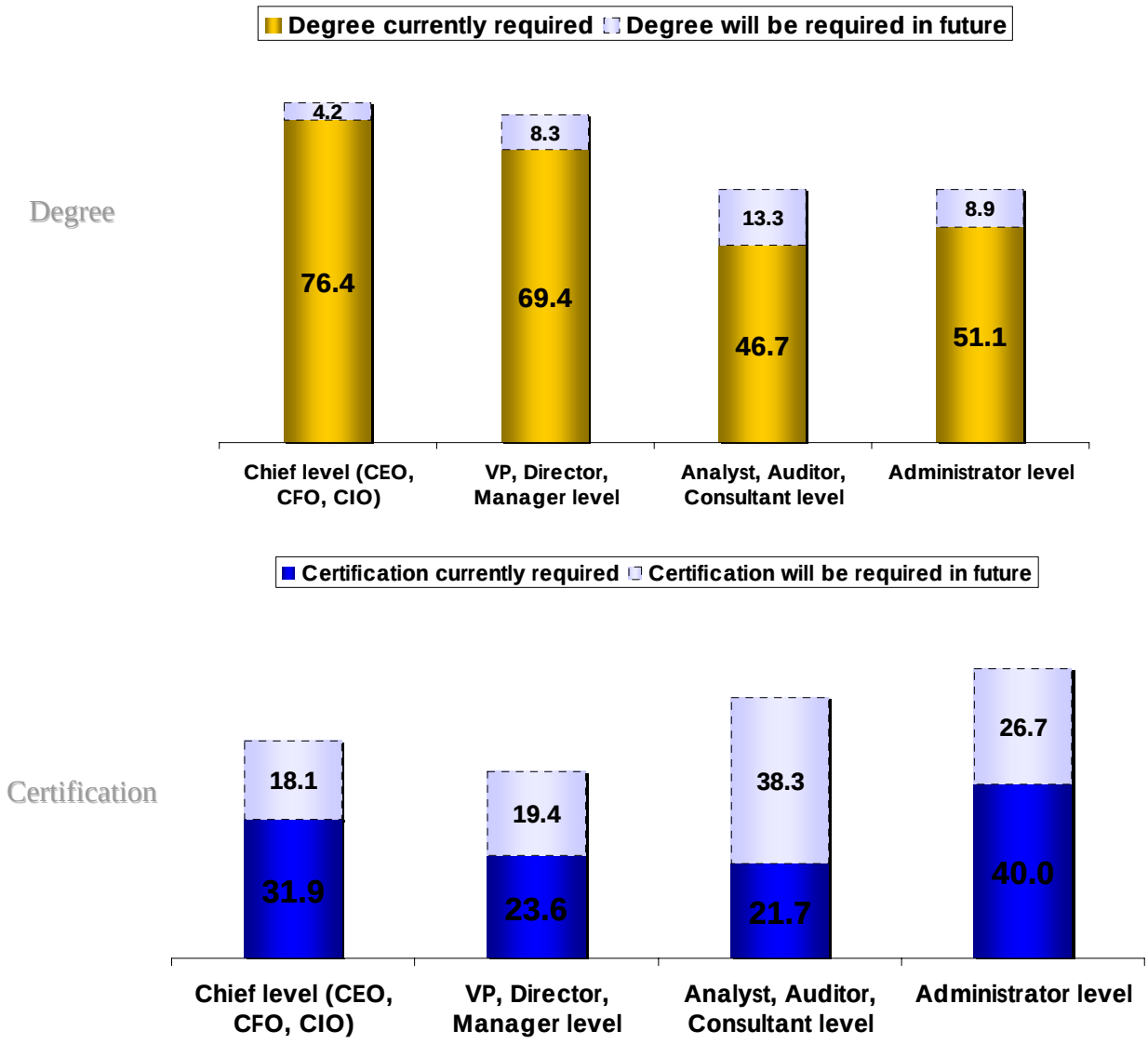




Need for Degree and Certification in Information Security Professions

- 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?

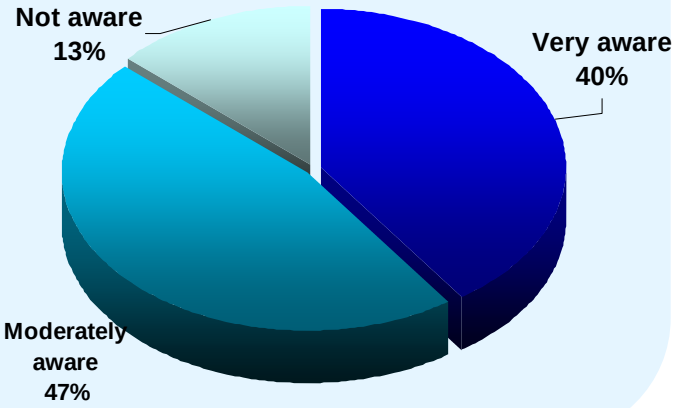


Awareness for Information Security degrees/certifications

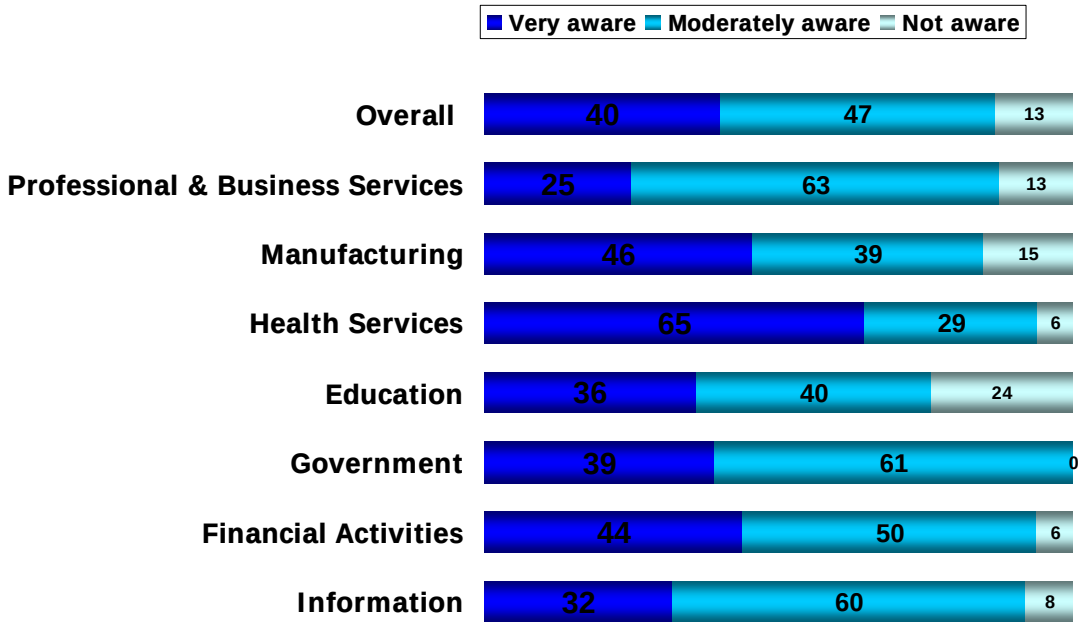
- Approximately 87% say they are **very** to **moderately aware** of ways to get information security degrees and/or certifications. Approximately two-thirds (61%) claim to be aware of *some type* of specific IS certification and/or degree program.
- Forty-eight percent associate this program with "educational 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?



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



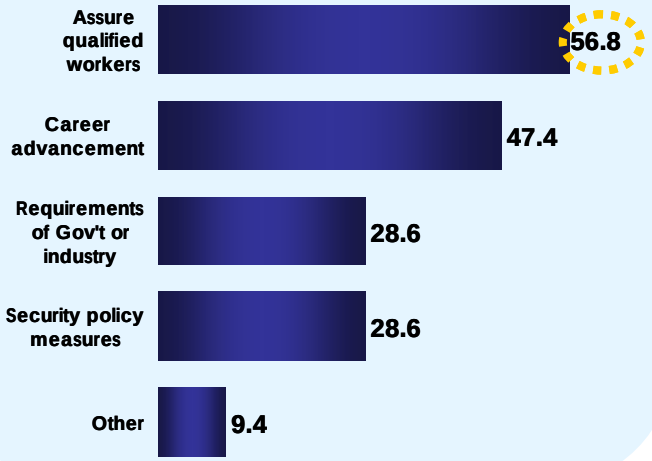
Perceptions surrounding Information Security degrees/certifications

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

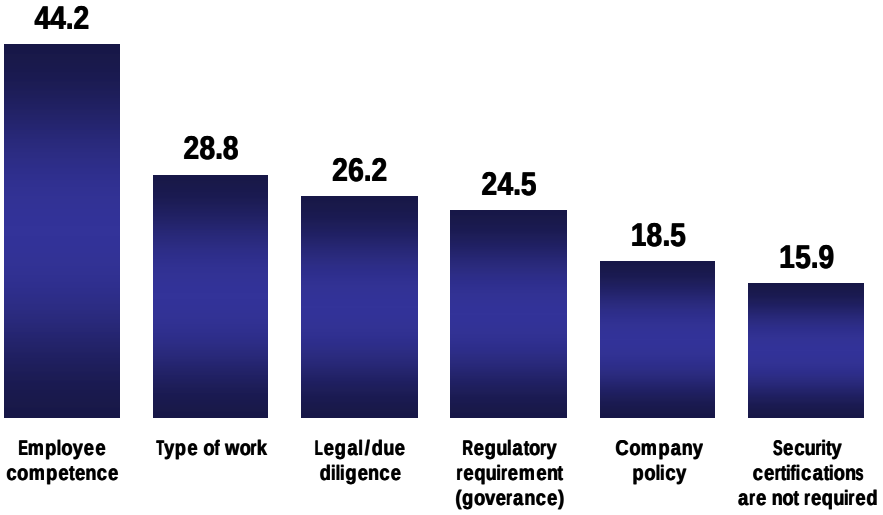
- **The primary reasons** employers would "hire" an information security professional with a degree or certification would be:
  1. Employee competence
  2. Type of work
  3. Legal/due diligence
  4. Regulatory requirements

Reasons to obtain:

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



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



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%)

Appendix

Michigan Career Outlook 2002-2012				
Position	Michigan Projected % Job Growth rate 2002-2012(1)	SE Michigan Projected % Job Growth rate 2002-2012(1)		Education/training required (1)
Computer & Information Systems Managers	28.5%	27.1%		Bachelors or higher + work experience
Computer Software Engineers, Systems Software	45.3%	42.7%		Bachelors or higher
Computer Software Engineers, Applications	36.5%	36.0%		Bachelors or higher
Computer Systems Analysts	31.5%	30.3%		Bachelors or higher
Network Systems and Data Communication Analysts	45.6%	49.7%		Bachelors
Network and Computer Systems Administrators	30.2%	28.6%		Bachelors

(1) Michigan Career Outlook, through 2012, Bureau of Labor Market Information & Strategic Initiatives, www.michigan.gov/lmi

Michigan Job Growth compared to Southeast Michigan Job Growth to 2012				
Position	Job Growth to 2012 for Michigan	Job Growth to 2012 for Southeast MI*	Southeast MI as a % of Total Michigan	Education/training required (1)
Computer & Information Systems Managers	2,085	1,185	56.8%	Bachelors or higher + work experience
Computer Software Engineers, Systems Software	2,220	1,840	82.9%	Bachelors or higher
Computer Software Engineers, Applications	3,510	2,125	60.1%	Bachelors or higher
Computer Systems Analysts	5,450	3,840	70.5%	Bachelors or higher
Network Systems and Data Communication Analysts	1,465	835	57.0%	Bachelors
Network and Computer Systems Administrators	1,945	1,145	58.9%	Bachelors
*Southeast MI (Lapeer, Macomb, Monroe, Oakland, St. Clair, Wayne				

Verbatim

Q17. What reason(s) would you hire an information security degreed/certified professional? Base: Other

- Customer confidence
- Customer requirement
- Did not include additional information
- Don't have anybody
- Experiences
- Knowledge of industry standards
- Needs of clients
- None
- Security certificate not required
- Security Software Competence
- Sign of progression in career
- State policy
- We promote within from IT professional staff
- We wouldn't hire, we outsource them

19. What specific training, qualifications and/or degrees/certifications will they need?

- 1-3 yrs info sec experience, bachelors, CISSP, CISA, CISM
- A+ Certification and maybe a CISP certificate
- Artificial intelligence degrees
- Associates and/or CISSP,CISM,CDRP
- Associates Degree with specialization
- BA
- BA or Security Cert (CISSP)
- BA, perhaps CISA & CISSP
- BA, Security Certificate
- BA/BS and/or CISSP
- Bachelor degree for any position
- Bachelor Degree, 5+ years experience
- Bachelors
- Bachelors
- Bachelors
- Bachelors
- Bachelors
- Bachelors Degree, CISSP
- Bachelors Degree, industry standard security training
- Bachelors of Science & 10+ years of experience with comparably sized company
- Bachelor's with minimum 32 hrs. of computer-related core subject matter
- Bachelors, CISSP, CISA, one vender neutral cert.
- BS/BA
- BS/CISSP
- CCNA, Security +, Server 2003, Network +
- Certification
- Certification
- CIAC
- Cisco, CCNA, Pix
- CISP, CCSE, CCNP
- CISSP, Bachelor

- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP
- CISSP, BA
- CISSP, CCNP, ITIL
- CISSP, CISA
- CISSP, CISA
- CISSP, CISA
- CISSP, CISA, BBA
- CISSP, CISA, NSA4011, MSBIT (masters degree)
- CISSP, CISM
- CISSP, CISM
- CISSP, CSSP
- CISSP, or technical cert is OS, Network, ect
- CISSP,CCIE-SECURITY
- CISSP,CISA,CIA
- CISSP/CCNA
- CISSP/Forensics
- CISSP; Bachelor Degree
- Computer Science, CISSP
- Degree + experience
- Degree required
- Depends on area/agency/tasks
- Depends?
- Do not know yet, to be determined
- Don't Know
- Experience
- Experience
- Hands on experience; AT certifications; Knowledge of Java, Ctt, Php (future degree)
- I don't look at certificates, I look at experience
- Industry specific degree
- Industry standards plus experience
- IT Degree and experience
- It depends on position, Bachelors and certification
- IT Security Degrees
- Just previous experience
- Masters degree, MCSE, Cisco training, depending on position
- Masters, CISSP
- MCSE, BA
- MCSE, Bachelors Degree
- Microsoft CBCO
- Minimum of a 4 year degree + 2 month in house training
- Network specialist, data evaluation

- None are required, MCSA would be desirable
- None required
- None, just experience
- Not sure
- Organization standards
- Product Specific PLM
- Project Management experience
- security +
- Security tt
- Some certifications, college level computing courses
- They would need to be certified, with what I don't know. I'm not the person who hires and fires
- To be determined

Q21. Are there any other IA training/vocational programs you are aware of?

- Boot Camp
- ISSA, ISACA, RMP
- Microsoft
- Microsoft Novell
- Netware, Microsoft, Proxima, Cisco
- No
- None
- Not really
- Private organizations
- SANS
- Through mail or email
- Vendor class
- Vocation
- What is IA?
- Woruich(or Norwich) University, National Security Agency

Laws and regulations governing Information Security

- FERPA
- HIPAA

  "The **Health Insurance Portability and Accountability Act** (**HIPAA**) was enacted by the U.S. Congress in 1996. According to the Centers for Medicare and Medicaid Services' (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the US health care system."

- Gramm-Leach-Bliley Act of 1999
- ISO 27001
- PCI
- SAS70
- Sarbanes-Oxley Act of 2002 (also called SOX)

  "The **Sarbanes-Oxley Act of 2002** (Pub. L. No. 107-204, 116 Stat. 745, also known as the **Public Company Accounting Reform and Investor Protection Act of 2002** and commonly called **SOX** or **Sarbox**; July 30, 2002) is a United States federal law passed in response to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Peregrine Systems and WorldCom (recently MCI and currently now part of Verizon Businesses). The legislation is wide ranging and establishes new or enhanced standards for all U.S. public company boards, management, and public accounting firms."

Professional organizations

Verbatim from their web-sites

"The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government.

The ISSA international board consists of some of the most influential people in the security industry, with representatives from Dell Computer Corporation, EDS, Forrester Research Inc., Symantec and Washington Mutual. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as The Global Voice of Information Security.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved." www.issa.org

"ISACA has more than 170 chapters established in over 70 countries worldwide, and those chapters provide members education, resource sharing, advocacy, professional networking and a host of other benefits on a local level. Find out if there's a chapter near you.

In the three decades since its inception, ISACA has become a pace-setting global organization for information governance, control, security and audit professionals. Its IS auditing and IS control standards are followed by practitioners worldwide. Its research pinpoints professional issues challenging its constituents. Its Certified Information Systems Auditor (CISA) certification is recognized globally and has been earned by more than 50,000 professionals since inception. The Certified Information Security Manager (CISM) certification uniquely targets the information security management audience and has been earned by more than 6,000 professionals. It publishes a leading technical journal in the information control field, the *Information Systems Control Journal*. It hosts a series of international conferences focusing on both technical and managerial topics pertinent to the IS assurance, control, security and IT governance professions. Together, ISACA and its affiliated IT Governance Institute lead the information technology control community and serve its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment." www.isaca.org

SANS

"SANS is the most trusted and by far the largest source for information security training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - Internet Storm Center.

The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding

solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community."

Many of the valuable SANS resources are free to all who ask. They include the very popular Internet Storm Center (the Internet's early warning system), the weekly news digest (NewsBites), the weekly vulnerability digest (@RISK), flash security alerts and more than 1,200 award-winning, original research papers." www.sans.org

"The International Information Systems Security Certification Consortium, or (ISC)²® , is the internationally recognized *Gold Standard* for educating and certifying information security professionals throughout their careers. We've certified over 42,000 information security professionals in more than 110 countries.

Founded in 1989 by industry leaders, (ISC)² issues the Certified Information Systems Security Professional (CISSP ®) and related concentrations: Information Systems Security Architecture Professional (ISSAP ®), Information Systems Security Management Professional (ISSMP ®) and Information Systems Security Engineering Professional (ISSEP ®); the Certification and Accreditation Professional (CAP CM); and the Systems Security Certified Practitioner (SSCP ®) credentials to those meeting the necessary competency requirements. Several of (ISC)²'s credentials meet the stringent requirements of ANSI/ISO/IEC Standard 17024, a global benchmark for assessing and certifying personnel.

(ISC)² also offers a portfolio of education products and services based upon (ISC)²'s CBK ®, a compendium of industry best practices for information security professionals, and is responsible for the annual (ISC)² Global Information Security Workforce Study." www.isc2.org

The High Technology Crime Investigation Association (HTCIA) is designed to encourage, promote, aid and affect the voluntary interchange of data, information, experience, ideas and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership. http://www.htcia.org/

COMPUTER SECURITY INSTITUTE

"Computer Security Institute serves the needs of Information Security Professionals through membership, educational events, security surveys and awareness tools. Joining CSI provides you with high quality CSI publications, discounts on CSI conferences, access to on-line archives, career development, networking opportunities and more.

CSI holds two conferences annually: CSI NetSec in June and the Annual Computer Security Conference and Exhibition in the Fall. These conferences are targeted both to those entering the field, as well as to experienced practitioners and draw attendees from around the world.

CSI publishes the annual CSI/FBI Computer Crime & Security Survey which attracts widespread media attention, and holds an annual Security Survey Roadshow in various cities. CSI Awareness offers products and training to help improve awareness that includes Frontline end user awareness newsletter, World Security Challenge web-based awareness training, awareness peer groups and more. Private training from CSI is also available for organizations." www.gocsi.com

Certifications

Verbatim adopted directly from www.wikipedia.com

CISSP (Certified Information Systems Security Professional)

"Certified Information Systems Security Professional (**CISSP**) is a vendor-neutral certification governed by the International Information Systems Security Certification Consortium (ISC)^2. It is considered one of the premiere Information Security certifications. In granting the CISSP certification (ISC)^2 operates in conformance with the requirements of the International Organization for Standardization (ISO) standard ISO 17024:2003 for certifying individuals.

The CISSP test includes information from 10 different domains which comprise the (ISC)^2 Common Body of Knowledge® (CBK). According to its sponsor (ISC)^2, applicants for the CISSP must have one of the following to qualify:

- A minimum of four years of direct full-time security professional work experience in one or more of the ten domains of the CBK®
- Three years of direct full-time of the CBK® with a four-year college degree.
- A Master's Degree in Information Security from a National Center of Academic Excellence (CAE) can substitute for one year toward the four-year requirement.

Individuals who achieve the CISSP are required to complete 120 Continuing Professional Education (CPE) units over a period of 3 years in order to maintain the certification. CPE's can be earned several ways, including attending seminars, achieving additional certifications or degrees, publishing work related to information security. If a CISSP does not maintain 120 CPEs in 3 years, he/she will need to retake the CISSP exam in order to maintain active status.

The CISSP has been described as covering Information Security topics "A mile wide, and an inch deep." The certification demonstrates a wide range of expertise in a variety of topics as listed below.

The CBK® includes:

- Access Control
- Application Security
- Business Continuity and Disaster Recovery Planning
- Cryptography
- Information Security and Risk Management
- Legal, Regulations, Compliance and Investigations
- Operations Security
- Physical (Environmental) Security
- Security Architecture and Design
- Telecommunications and Network Security

For experienced information security professionals with an (ISC)^2 credential in good standing, (ISC)^2 Concentrations demonstrate their acquired rigorous knowledge of select CBK® domains. Passing a concentration examination demonstrates proven capabilities and subject-matter expertise beyond that required for the CISSP or SSCP credentials.

Current Concentrations for CISSPs include the:

- ISSAP, Concentration in Architecture
- ISSEP, Concentration in Engineering
- ISSMP, Concentration in Management

Although the CISSP is widely considered to be the de facto certification for information security professionals, it has also been criticized by some parties:

- Being an "inch deep and a mile wide" means that the test has little or no depth, and passing it may prove only that a person is good at memorizing facts and passing examinations- although the requirement that candidates submit proof of four years' experience in the field does address this issue to some extent.
- It sometimes tests on outdated information (for instance, the CISSP exam as of 2006 still sometimes asks questions about 10BASE2 Ethernet, which has not been widely used since the 1990s).
- The test is formulated so that candidates are asked to choose the best answer from among a group, rather than an actual correct answer. Some feel that this is a form of "trick" question, and really just tests attention to detail, rather than the subject matter.
- Some questions given on CISSP tests, and information in the CBK® itself, may be technically inaccurate, skewed, or incomplete. For instance, the *Official (ISC)2 Guide to the CISSP Exam*, based on the CBK®, says that all host-based intrusion detection systems work by reading audit logs -- completely ignoring the fact that the most common such system used today is probably Tripwire, which does not read audit logs. Critics charge that inaccuracies and wild blanket statements such as this are too common within the CBK®.
- The requirement to be sponsored by another CISSP means that the qualification is not entirely knowledge- and competence-based, but also involves knowing someone willing to provide sponsorship, effectively keeping it within the 'club' (however, if you do not know a CISSP willing to sponsor you, (ISC)2 allows a senior level (CIO, CTO, CSO) manager to attest to your background and experience in a written statement).

CISM (Certified Information Systems Auditor)

"Certified Information Systems Auditor (**CISA**) is a professional certification sponsored by the Information Systems Audit and Control Association. Candidates for the certification must meet certain requirements, including passing an examination, before qualification is awarded. Experience in auditing information systems is required.

The CISA certification was established in 1978 for several reasons:

1. Develop and maintain a tool that could be used to evaluate an individuals' competency in conducting information system audits.

2. Provide a motivational tool for information systems auditors to maintain their skills, and monitor the success of the maintenance programs.

3. Provide criteria to help aid management in the selection of personnel and development.

The first CISA examination was administered in 1981, and registration numbers have grown each year. The exam is now offered in 11 languages at more than 200 locations worldwide. In 2005, Information Systems Audit and Control Association, or ISACA, announced that the exam would be offered in both June and December, starting in 2005. Previously, the exam had only been administered annually, in June. Over 48,000 candidates have earned the CISA designation.

The CISA certification has been recognized with ANSI accreditation, along with the CISM certification- both of these certifications are managed by ISACA. It is one of the few certifications formally recognized by the US Department of Defense in their Information Assurance Technical category.

Candidates for a CISA certification must pass the examination, agree to adhere to ISACA's Code of Professional Ethics, submit evidence of a minimum of five years of professional IS auditing, control, or security work, and abide by a program of continuing professional education. Substitutions and waivers of such experience may be obtained as follows: *(From the ISACA CISA Certification site [1])*

- A maximum of one year of information systems experience OR one year of financial or operational auditing experience can be substituted for one year of information systems auditing, control, or security experience.

- 60 to 120 completed college semester credit hours (the equivalent of an Associate or Bachelor degree) can be substituted for one or two years, respectively, of information systems auditing, control or security experience.

- Two years as a full-time university instructor in a related field (e.g., computer science, accounting, information systems auditing) can be substituted for one year of information systems auditing, control or security experience.

CCSE (Computing Curriculum Software Engineering)

The **Software Engineering 2004** (**SE2004**) —formerly known as **Computing Curriculum Software Engineering** (**CCSE**)— is a document that provides recommendations for undergraduate education in software engineering.

SE2004 was initially developed by a steering committee between 2001 and 2004. Its development was sponsored by the Association for Computing Machinery and the IEEE Computer Society.

Important components of SE2004 include the Software Engineering Education Knowledge, a list of topics that all graduates should know, as well as a set of guidelines for implementing curricula and a set of proposed courses.

CCNA (Cisco Certified Network Associate)

Authorized training is provided globally by Cisco Learning Partners. Also available are self-study guide by Cisco Press. Additional resources and tools to aid in preparing for the certification are available on the CCNA Prep Center, www.cisco.com/go/prepcenter.

The test presents between 50 & 60 questions within a 90 minute period; The test includes multiple choice questions (including many multiple-answer questions, e.g. 'which three of these five options'), matching questions, and simulated 'lab' questions that provide a virtual network consisting of several routers and switches to test troubleshooting skills. The test is scored from 300 to 1000 marks, with 300 being the minimum marks that everyone is granted. A grade of 84.9% (849 out of 1000) is required to pass. Pass or fail grade is indicated immediately on completion of test.

There is also a two-test option using the INTRO and ICND tests. This allows the candidate to focus on certain subjects. INTRO covers modules 1 & 2 of the CCNA curriculum and ICND covers 3 & 4.

The certification is valid for three years; at that time a CCNA holder must either re-take the certification exam or take an exam for one of the Professional or Specialist level certifications, such as CCNP. At one point, the CCNA re-certification exam was different from the CCNA exam, but this is no longer the case.

Internationally there is also the Cisco Academy Programme, which brings the CCNA to learners in all nations and all communities.[1]

CCNP (Cisco Certified Network Professional)

The CCNP is considered proof of having the ability to work with medium-sized networks (between 100 and 500 end devices) and with technology such as QoS, broadband, VPNs, and security-minded features. To acquire a CCNP, one must pass four tests, and either re-certify or upgrade to a CCIE every three years. (The CCNA is a prerequisite for CCNP, CCIE does not have any prerequisites.)

CCDP (Cisco Certified Design Professional)

An advanced network design certification provided by Cisco Systems, Inc. Candidates for the certification are tested for advanced knowledge of Cisco devices and the way to interconnect them. This certification is considered a professional level certificate by Cisco Systems. (The CCNA and CCDA are prerequisites.)

CCSP (Cisco Certified Security Professional)

An advanced network security certification. Candidates for the certification are tested for advanced knowledge of various Cisco security products. To attain this certification several tests must be passed in the areas of VPN, IDS, PIX firewall, Secure IOS, the Cisco SAFE, as well as having a CCNA or equivalent (CCNP or CCIE).

CCIP (Cisco Certified Internetwork Professional)

A professional certification covering the end-to-end protocols used in large scale networks. To attain this certification tests must be passed in the areas of routing, BGP, MPLS and Quality of service.

CCVP (Cisco Certified Voice Professional

A certification covering all aspects of IP Telephony/VOIP networks and applications. To attain this certification, five tests must be passed in the areas of Quality of service, Cisco VoIP, IP Telephony Troubleshooting, Cisco IP Telephony, and Gateway Gatekeeper.

CCIE (Cisco Certified Internetwork Expert)

The expert-level certification is the It is the highest level of professional certification that Cisco provides. There are 5 active CCIE tracks, as below. As of December 1, 2006 there are 14,141 people with active CCIE certifications.[2] The CCIE is comprised of a written exam and a "lab" exam (each in the specific area of the chosen track). The written exam is required to take the lab exam, and has a cost of $300 USD per attempt. Upon successful completion of the written exam, the candidate then qualifies to register for the lab portion. The CCIE Lab is currently $1,250 USD per attempt. CCIE Labs are offered only at Cisco locations. There are currently 10 locations to

take the "lab" exam worldwide. The locations are Bangalore; Beijing; Brussels; Dubai; Hong Kong; Research Triangle Park, NC; San Jose, CA; Sao Paulo; Sydney; and Tokyo.

The Lab is an 8-hour hands-on exam designed to demonstrate that the candidate not only knows the theory, but is also able to practice it. Many prospective CCIEs need multiple attempts to pass the lab exam.[3]

There are no formal prerequisites for the CCIE exam, but Cisco recommends one has at least 3 - 5 years experience in networking before attempting to become a CCIE. CCIE was the first *Cisco Certified* qualification, and as such there were no other certifications that could be taken prior. The development of the associate and professional certifications was due to recognition of the fact that a CCIE is overkill for many networking personnel, and also for the vast majority of businesses who employ such people, and that certifications needed to be offered at lower levels. Despite the development of the lower certifications, Cisco has chosen not to make them formal requirements for the CCIE certification.

Glossary

All definitions provided are verbatim adopted from pages sourced through Wikipedia, www.wikipedia.com

Access Control Systems and Methodology

Limiting access to information system resources only to authorized users, programs, processes, or other systems. **Access control list (ACL):** Mechanism implementing discretionary and/or mandatory access control between subjects and objects. **Access control mechanism:** Security safeguard designed to detect and deny unauthorized access and permit authorized access in an IS. **Access level**: Hierarchical portion of the security level used to identify the sensitivity of IS data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. (See category.) **Access list (IS):** Compilation of users, programs, or processes and the access levels and types to which each is authorized. (COMSEC) Roster of individuals authorized admittance to a controlled area.

Application and System Development Security

Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Audits

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Business Continuity

Continuity of operations plan. A plan for continuing an organization's (usually a (COOP) headquarters element) essential functions at an alternate site and performing those functions for the duration of an event with little or no loss of continuity before returning to normal operations.

Business Continuity Planning (**BCP**) is an interdisciplinary peer mentoring methodology used to create and validate an exercised logistical plan for how an organization will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster or extended disruption. For open source BCP "how-to" guidelines, see Wikibooks - Business and economics. BCP may be a part of an organizational learning effort that helps reduce operational risk associated with lax information management controls. This process may be integrated with improving information security and corporate reputation risk management practices.

Corporate Governance

Corporate governance is the set of processes, customs, policies, laws and institutions affecting the way a corporation is directed, administered or controlled. Corporate governance also includes the relationships among the many players involved (the stakeholders) and the goals for which the corporation is governed. The principal players are the shareholders, management and the board of directors. Other stakeholders include employees, suppliers, customers, banks and other lenders, regulators, the environment and the community at large.

Recently there has been considerable interest in the corporate governance practices of modern corporations, particularly since the high-profile collapses of large US firms such as Enron Corporation and Worldcom.

The term corporate governance has come to mean two things.

- The processes by which companies are directed and controlled.
- A field in economics, which studies the many issues arising from the separation of ownership and control.

The corporate governance structure spells out the rules and procedures for making decisions on corporate affairs. It also provides the structure through which the company objectives are set, as well as the means of attaining and monitoring the performance of those objectives. Corporate governance is used to monitor whether outcomes are in accordance with plans and to motivate the organization to be more fully informed in order to maintain or alter organizational activity. Corporate governance is the mechanism by which individuals are motivated to align their actual behaviors with the overall participants.

Disaster Recovery Planning

Disaster Recovery Planning: Provides for the continuity of system operations after a disaster.

A **Disaster recovery** plan covers the data, hardware and software critical for a business to restart operations in the event of a natural or human-caused disaster. It should also include plans for coping with the unexpected or sudden loss of key personnel, although this is not covered in this article, the focus of which is data protection. With the rise in information technology and the reliance on business-critical data, the landscape has changed in recent years in favor of protecting irreplaceable data. This is especially evident in information technology, with most large computer systems backing up digital information to limit data loss and to aid data recovery.

It is believed that some companies spend up to 25% of their budget on disaster recovery plans; however, this is to avoid bigger losses. Of companies that had a major loss of computerized records, 43% never reopen, 51% close within two years, and only 6% will survive long-term. (Cummings, Haag & McCubbrey 2005.)

The current data protection market is characterized by several factors:

- Rapidly changing customer needs that are driven by data growth, regulatory issues and the growing importance to access data quickly by retaining it online.
- An ever-shrinking time frame for backing up data, which is burdening conventional tape backup technologies.

As the disaster recovery market continues to undergo significant structural changes, the shift presents opportunities for next-generation startup companies that specialize in business continuity planning and offsite data protection.

Information Forensics

Information Forensics is the science of investigation into systemic processes that produce information. Systemic processes utilize primarily computing and communication technologies to capture, treat, store and transmit data. Manual processes complement technology systems at every stage of system processes; e.g. from data entry to verification of computations, and management of communications to backing-up information reports. In context, both technology and manual systems, with systemic processes that are either proprietary by design or evolved inconsequentially, constitute the enterprise Information System.

The complexity of enterprise business systems, in particular those augmented with technology and legacy systems, often are susceptible to fraud, abuse, mistakes, and sabotage.

Information forensic investigation dwells into the aspects of creation, operation and evolution of the enterprise information system. Specifically, investigation focuses on causal factors and processes that govern the life cycle implementation of such systems. Forensic investigation may be initiated when a system is suspect or compromised; generally, investigation occurs when a system fails. Investigations normally concentrate on specific problem areas or components of a system; the intricacies of business systems, costs and resources available, often preclude detailed examination of the whole information system. Nevertheless, bringing about scientific examination of facts when problems occur is not only prudent, but necessary for the court of law. The methodological approach to investigation at present is the subject of research interest and topical development.

The following discourse highlights some of the issues in Information Forensics that includes:

- Adherence to conventions
- Dealing with parties of interest
- Technology and systems design

Intrusion-prevention system

An **intrusion prevention system** is a computer security device that exercises access control to protect computers from exploitation. **Intrusion prevention** technology is considered by some to be an extension of intrusion detection (IDS) technology but it is actually another form of access control, like an application layer firewall. The latest Next Generation Firewalls leverage their existing deep packet inspection engine by sharing this functionality with an **Intrusion-prevention system**. Intrusion prevention systems (IPS) were invented in the late 1990s to resolve ambiguities in passive network monitoring by placing detection systems in-line. A considerable improvement upon firewall technologies, IPS make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. As IPS systems were originally a literal extension of intrusion detection systems, they continue to be related.

The first commercial IPS was the BlackICE product from NetworkICE Corporation. It provided host and in-line network IPS capabilities using protocol analysis as its core detection technique. The first products were BlackICE Desktop (a host-IPS for end-user systems) BlackICE Guard (an in-line network IPS) and BlackICE Sentry (a passive, IDS solution). NetworkICE was purchased in 2000 by Internet Security Systems (ISS). The BlackICE engine is still used in most ISS products, including the Proventia line of products.

Intrusion prevention systems may also serve secondarily at the host level to deny potentially malicious activity. There are advantages and disadvantages to host-based IPS compared with network-based IPS. In many cases, the technologies are thought to be complementary.

ISO/IEC 27001 (Information Security Management System)

ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. Its full name is *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements* but it is commonly known as "ISO 27001".

ISO 27001 is a certification standard specifying requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS. The requirements are defined in a structured, formal format suitable for compliance certification. It is intended to be used in conjunction with ISO 17799, the Code of Practice for Information Security Management, which lists security control objectives and recommends a range of specific security controls. Organizations that implement an ISMS in accordance with the best practice advice in ISO 17799 are likely simultaneously to meet the requirements of ISO 27001, but certification is entirely optional.

This standard is the first in a family of information security related ISO standards which are expected to be assigned numbers within the 27000 series. Others are anticipated to include:

- ISO/IEC 27000 - a vocabulary or glossary of terms used in the ISO 27000-series standards
- ISO/IEC 27002 - the proposed re-naming of existing standard ISO 17799
- ISO/IEC 27003 - a new ISMS implementation guide
- ISO/IEC 27004 - a new standard for information security measurement and metrics
- ISO/IEC 27005 - a proposed standard for risk management, potentially related to the current British Standard BS 7799 part 3
- ISO/IEC 27006 - a guide to the certification/registration process

ISO 27001 was based upon and replaced BS 7799 part 2 which was withdrawn.

The ISO 27000-series information security management standards align with other ISO management systems standard, such as those for ISO 9001 (quality management systems) and ISO 14001 (environmental management systems), both in terms of their general structure and in the nature of combining best practice with certification standards.

Certification of an organisation's ISMS against **ISO/IEC 27001** is one means of providing assurance that the certified organisation has implemented a system for the management of information security in line with the standard. Credibility is the key advantage of being certified by a respected, independent and competent third party. The assurance it provides gives confidence to management, business partners, customers and auditors that the organization is serious about information security management - not perfect, necessarily, but at least on the right path to continuous, managed improvement.

Organizations may be certified compliant with ISO 27001 by a number of accredited certification bodies worldwide. Certification against any of the recognized national variants of ISO 27001 (e.g. the Japanese version) by an accredited certification body is functionally equivalent to certification against ISO 27001 itself.

ISO/IEC 27002 (Code of Practice for Information Security Management)

The Code of Practice for information security management recommends the following be examined during a risk assessment: **security policy, organization of information security, asset management, human resources security, physical and environmental security, communications and operations management, access control, information systems acquisition, development and maintenance, information security incident management, business continuity management, and regulatory compliance.**

In broad terms the risk management process consists of:

1. Identification of assets and estimating their value. Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
2. Conduct a threat assessment. Include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
3. Conduct a vulnerability assessment, and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
4. Calculate the impact that each threat would have on each asset. Use qualitative analysis or quantitative analysis.
5. Identify, select and implement appropriate controls. Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.
6. Evaluate the effectiveness of the control measures. Insure the controls provide the required cost effective protection without discernable loss of productivity.

Risk management

Risk management is the process of measuring, or assessing, risk and developing strategies to manage it. Strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk. Traditional risk management focuses on risks stemming from physical or legal causes (e.g. natural disasters or fires, accidents, death, and lawsuits). Financial risk management, on the other hand, focuses on risks that can be managed using traded financial instruments.

The CISA Review Manual 2006 provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."* [4]

A risk assessment is carried out by a team of people who have knowledge of specific areas of the business. Membership of the team may vary over time as different parts of the business are assessed. The assessment may use a subjective **qualitative** analysis based on informed opinion, or where reliable dollar figures and historical information is available, the analysis my use **quantitative** analysis.

Security Architecture & Models

A **computer security model** is a scheme for specifying and enforcing security policies. A security model may be founded upon a formal model of access rights, a model of computation, a model of distributed computing, or no particular theoretical grounding at all.

Security Management Practices

Security management: In network management, the set of functions (a) that protects telecommunications networks and systems from unauthorized access by persons, acts, or influences and (b) that includes many subfunctions, such as creating, deleting, and controlling security services and mechanisms; distributing security-relevant information; reporting security-

relevant events; controlling the distribution of cryptographic keying material; and authorizing subscriber access, rights, and privileges.

Source: From Federal Standard 1037C and from MIL-STD-188

In a more general management context, **Security management** entails the identification of an organization's information assets and the development, documentation and implementation of policies, standards, procedures and guidelines. Management tools such as information classification, risk assessment and risk analysis are used to identify threats, classify assets and to rate system vulnerabilities so that effective control can be implemented.