EDUCAUSE Center for Applied Research

Information Technology Security: Governance, Strategy, and Practice

University of Bergen
March 31, 2004

Robert B. Kvavik

Presentation agenda

- Study background – Research methodology and respondent demographics
- Summary of findings – A snapshot of higher education’s IT security environment
- Lessons learned – Common themes that emerged from the research
- The changing environment – How IT security in higher education seems to be evolving

Study Background

Research Methodology

- Consultation with a select group of IT security leaders in higher education to identify and validate the most interesting research questions and hypotheses
- Literature review to identify and clarify the study's major elements and create a working set of hypotheses to be tested
- Quantitative survey with responses from 435 higher education institutions
- Qualitative telephone interviews with 42 technology executives, managers, and faculty members at 18 institutions
- Four in-depth case studies

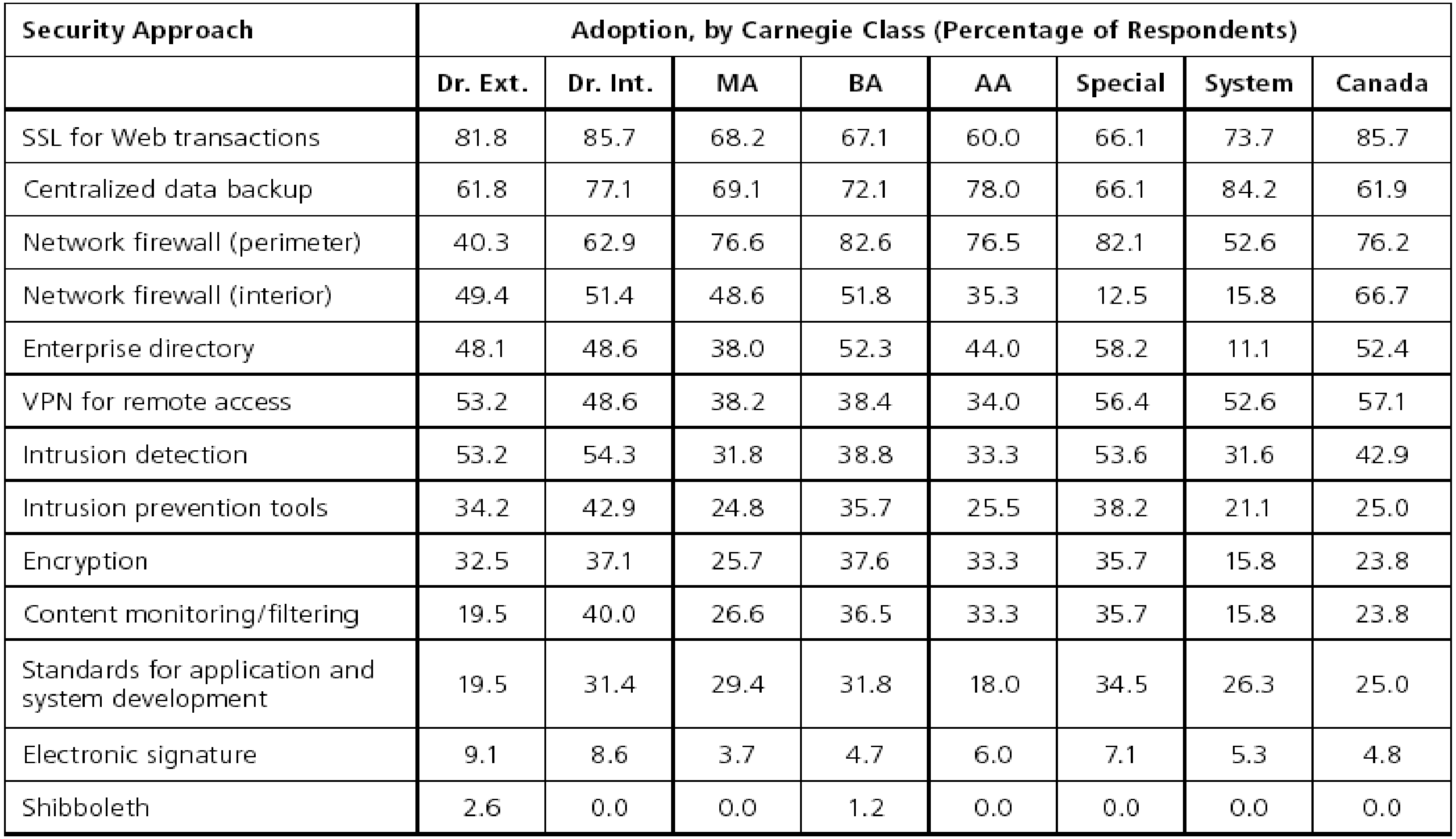
What do we mean by IT security?

- **Preserving *confidentiality*; protecting information from unauthorized use or disclosure**
- **Assuring information's *integrity*, including the accuracy and completeness of the data, through protection from unauthorized,unanticipated, and unintentional modification**
- **Making data *accessible* to authorized users on a timely basis**

- **Note: We chose to exclude certain topics often associated with IT security from our research, as many of these areas are broad enough to warrant separate study. These included disaster recovery, physical security, legal and ethical issues, legislative mandates, specific technologies by vendor, software licensing, and privacy.**

Summary of Findings

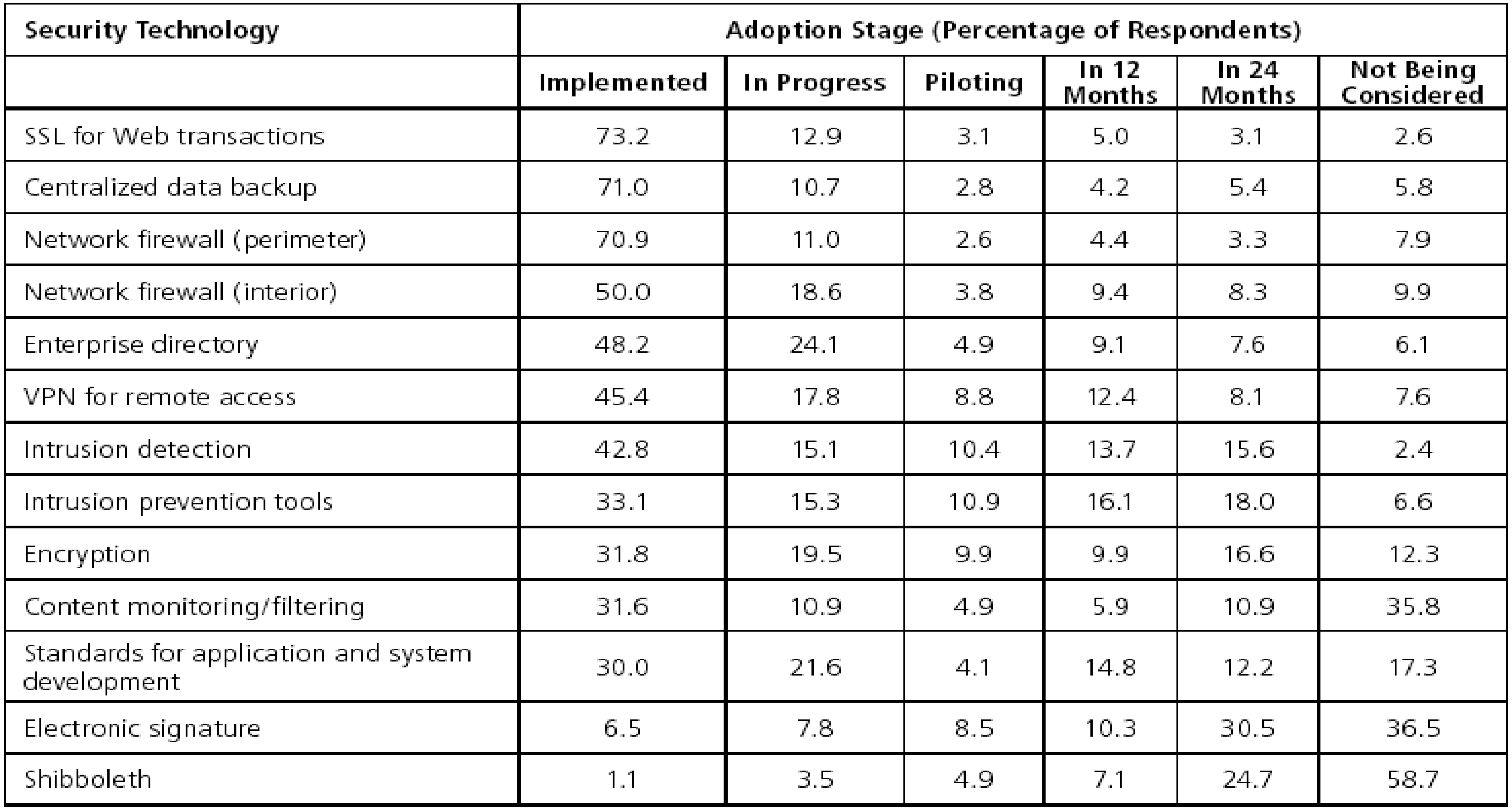
Security approaches in use varied by Carnegie class and institutional size



Security Approach	Adoption, by Carnegie Class (Percentage of Respondents)							
	Dr. Ext.	Dr. Int.	MA	BA	AA	Special	System	Canada
SSL for Web transactions	81.8	85.7	68.2	67.1	60.0	66.1	73.7	85.7
Centralized data backup	61.8	77.1	69.1	72.1	78.0	66.1	84.2	61.9
Network firewall (perimeter)	40.3	62.9	76.6	82.6	76.5	82.1	52.6	76.2
Network firewall (interior)	49.4	51.4	48.6	51.8	35.3	12.5	15.8	66.7
Enterprise directory	48.1	48.6	38.0	52.3	44.0	58.2	11.1	52.4
VPN for remote access	53.2	48.6	38.2	38.4	34.0	56.4	52.6	57.1
Intrusion detection	53.2	54.3	31.8	38.8	33.3	53.6	31.6	42.9
Intrusion prevention tools	34.2	42.9	24.8	35.7	25.5	38.2	21.1	25.0
Encryption	32.5	37.1	25.7	37.6	33.3	35.7	15.8	23.8
Content monitoring/filtering	19.5	40.0	26.6	36.5	33.3	35.7	15.8	23.8
Standards for application and system development	19.5	31.4	29.4	31.8	18.0	34.5	26.3	25.0
Electronic signature	9.1	8.6	3.7	4.7	6.0	7.1	5.3	4.8
Shibboleth	2.6	0.0	0.0	1.2	0.0	0.0	0.0	0.0

- BA institutions were twice as likely as doctoral extensive institutions to have perimeter firewalls
- Use of VPNs for remote access was substantially higher at larger institutions
- 83% of doctoral institutions used SSL for web transactions, compared to 65% of other Carnegie classes

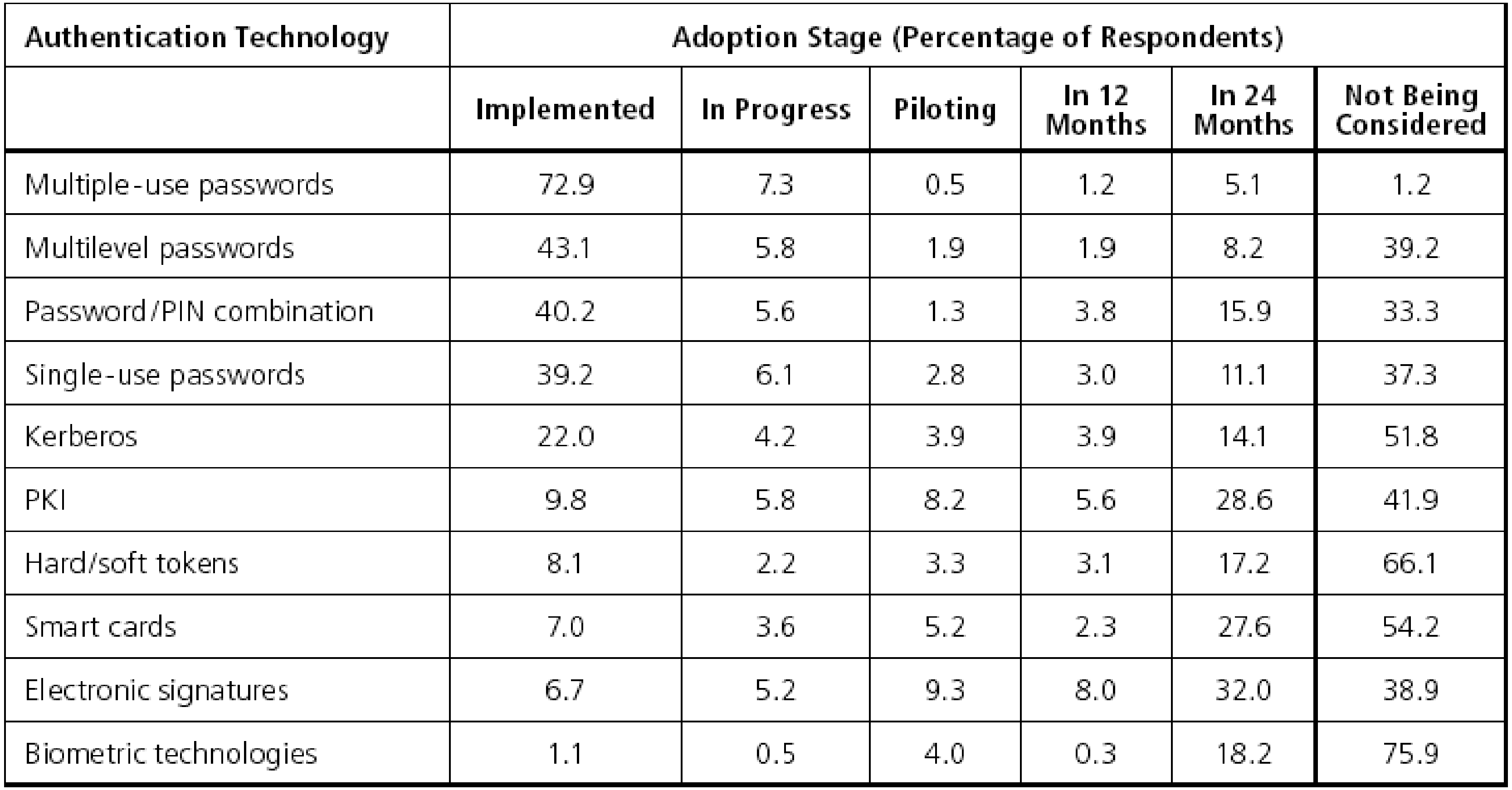
Higher education institutions continue to improve their IT security capabilities



Security Technology	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
SSL for Web transactions	73.2	12.9	3.1	5.0	3.1	2.6
Centralized data backup	71.0	10.7	2.8	4.2	5.4	5.8
Network firewall (perimeter)	70.9	11.0	2.6	4.4	3.3	7.9
Network firewall (interior)	50.0	18.6	3.8	9.4	8.3	9.9
Enterprise directory	48.2	24.1	4.9	9.1	7.6	6.1
VPN for remote access	45.4	17.8	8.8	12.4	8.1	7.6
Intrusion detection	42.8	15.1	10.4	13.7	15.6	2.4
Intrusion prevention tools	33.1	15.3	10.9	16.1	18.0	6.6
Encryption	31.8	19.5	9.9	9.9	16.6	12.3
Content monitoring/filtering	31.6	10.9	4.9	5.9	10.9	35.8
Standards for application and system development	30.0	21.6	4.1	14.8	12.2	17.3
Electronic signature	6.5	7.8	8.5	10.3	30.5	36.5
Shibboleth	1.1	3.5	4.9	7.1	24.7	58.7

- Use of established technologies, such as firewalls and SSL, will be pervasive within several years
- Use of newer tools, like enterprise directories and intrusion detection, appears to be growing rapidly
- Emerging technologies, like electronic signature and Shibboleth, are being adopted at a slower pace
- Higher education's use of many IT security tools lags behind their industry counterparts

Institutions are using a number of approaches to authenticate their users



Authentication Technology	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
Multiple-use passwords	72.9	7.3	0.5	1.2	5.1	1.2
Multilevel passwords	43.1	5.8	1.9	1.9	8.2	39.2
Password/PIN combination	40.2	5.6	1.3	3.8	15.9	33.3
Single-use passwords	39.2	6.1	2.8	3.0	11.1	37.3
Kerberos	22.0	4.2	3.9	3.9	14.1	51.8
PKI	9.8	5.8	8.2	5.6	28.6	41.9
Hard/soft tokens	8.1	2.2	3.3	3.1	17.2	66.1
Smart cards	7.0	3.6	5.2	2.3	27.6	54.2
Electronic signatures	6.7	5.2	9.3	8.0	32.0	38.9
Biometric technologies	1.1	0.5	4.0	0.3	18.2	75.9

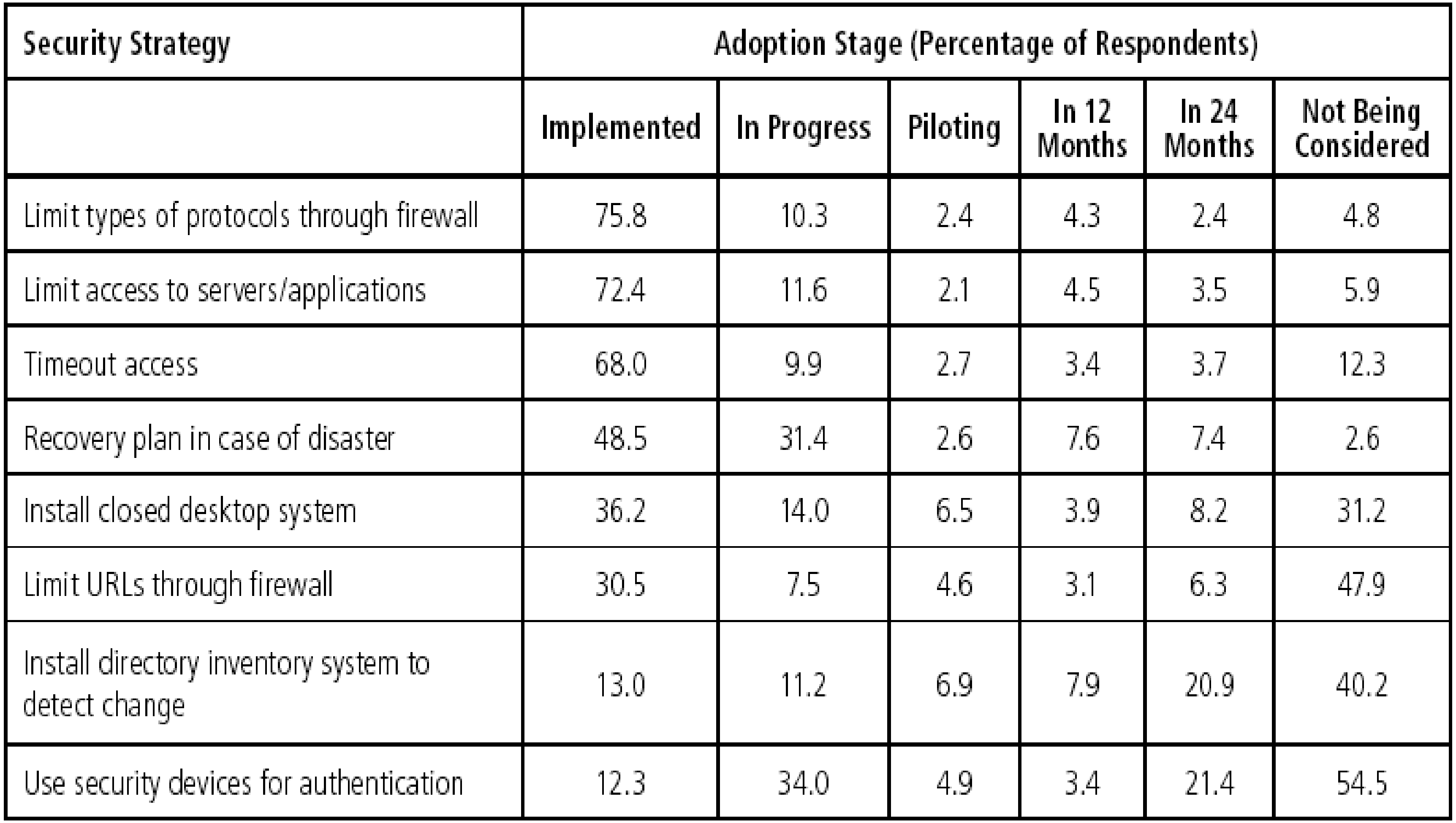
- All institutions reported using at least one form of authentication. Only 23% used one form, while 25% used two, and 17% used three. Several institutions reported using up to nine.
- 43% of doctoral extensive institutions reported using Kerberos, representing 49% of Kerberos users
- Doctoral institutions were more likely to use emerging technologies, but overall adoption remains low

Antivirus software is heavily used by most institutions

Asset Protected	% of Respondents
Desktop Operating Systems	97%
E-Mail Servers	92%
Application Servers	90%
Other Servers	88%

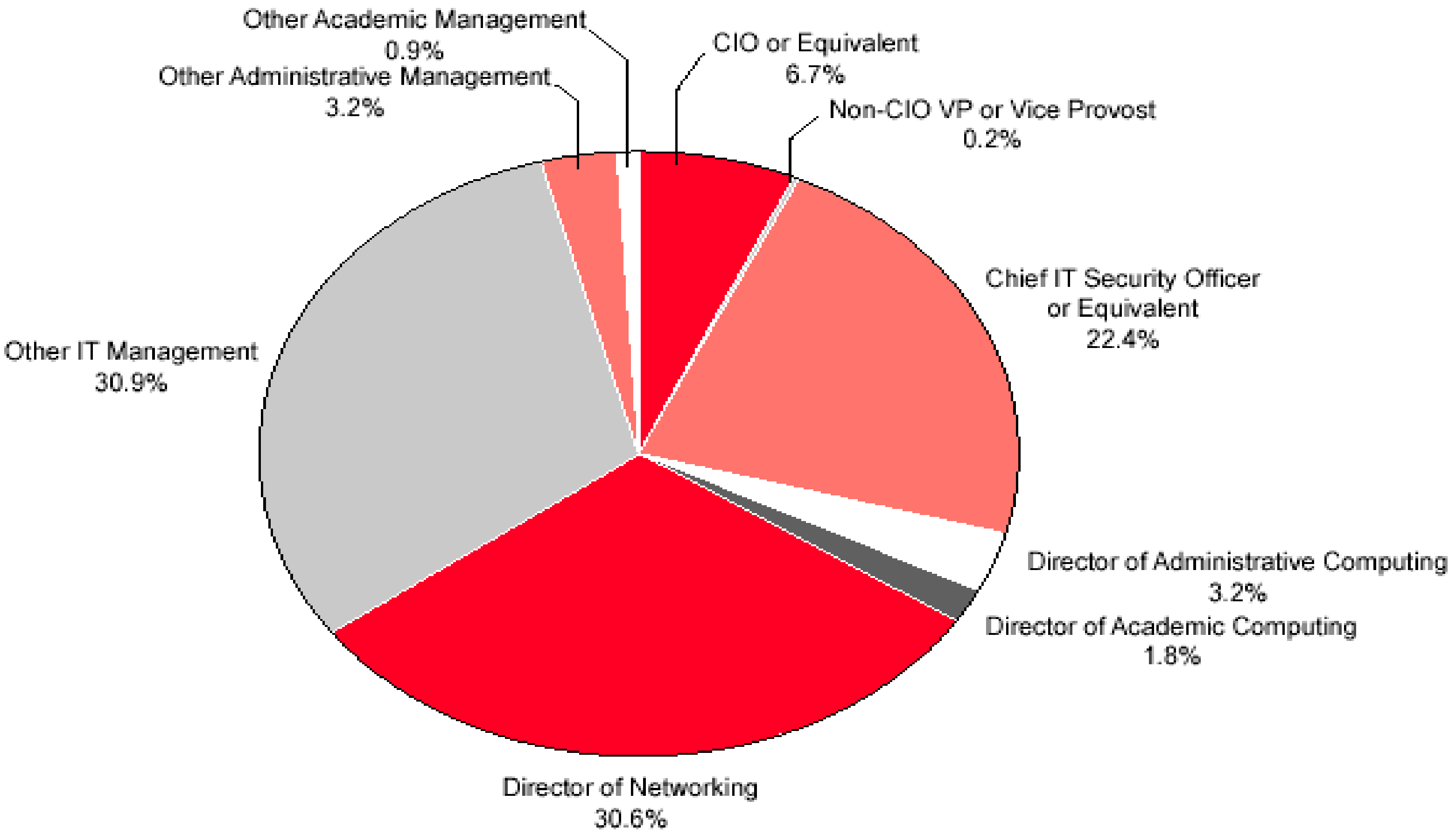
- 68% of respondents required that all institutionally owned systems have antivirus software installed to be connected to the network.
- This requirement was most prevalent at smaller institutions, with 87% of BA institutions requiring it, as opposed to only 30% of Dr. Ext. institutions
- Only 36% of respondents required non-institutionally owned systems to have antivirus software to connect to the network
- 98% of respondents have a site license for antivirus software, but this license covers personally owned computers at only 55% of institutions

Security strategies employed by institutions vary



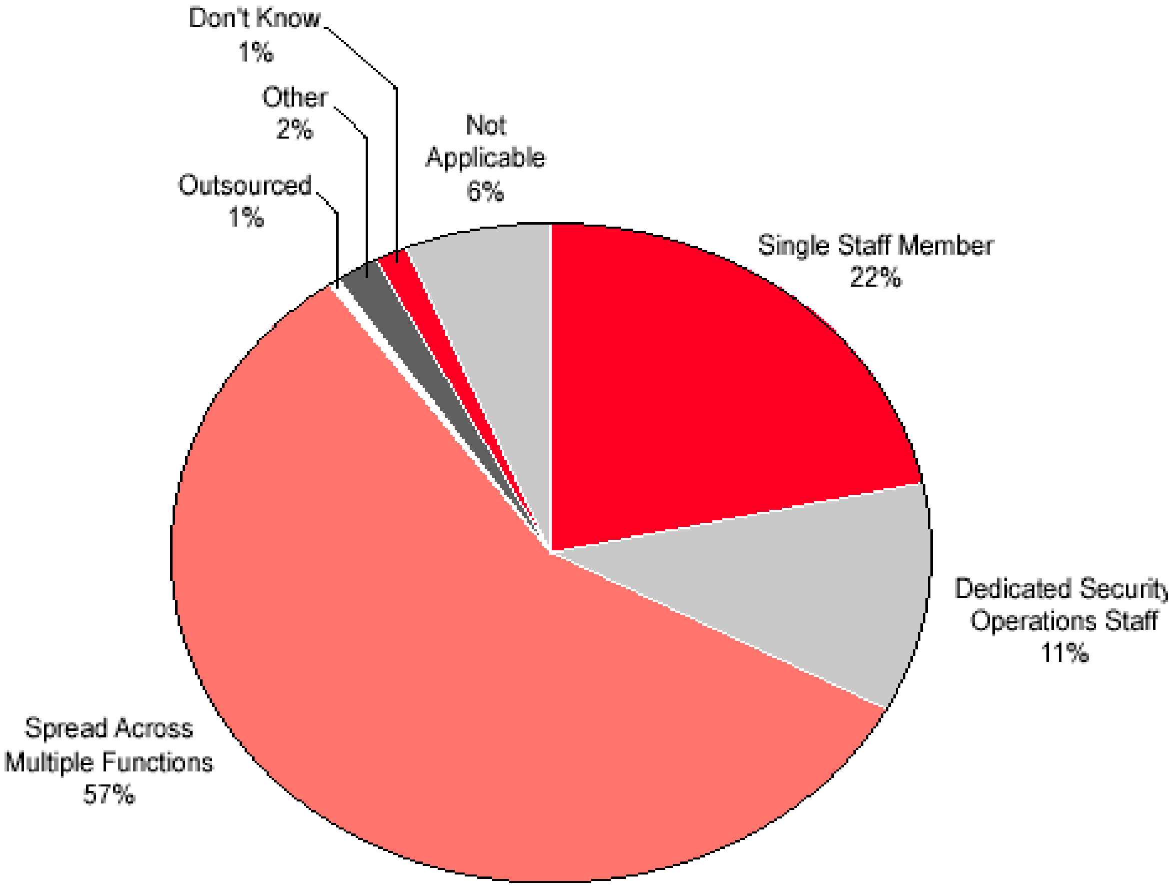
Security Strategy	Adoption Stage (Percentage of Respondents)					
	Implemented	In Progress	Piloting	In 12 Months	In 24 Months	Not Being Considered
Limit types of protocols through firewall	75.8	10.3	2.4	4.3	2.4	4.8
Limit access to servers/applications	72.4	11.6	2.1	4.5	3.5	5.9
Timeout access	68.0	9.9	2.7	3.4	3.7	12.3
Recovery plan in case of disaster	48.5	31.4	2.6	7.6	7.4	2.6
Install closed desktop system	36.2	14.0	6.5	3.9	8.2	31.2
Limit URLs through firewall	30.5	7.5	4.6	3.1	6.3	47.9
Install directory inventory system to detect change	13.0	11.2	6.9	7.9	20.9	40.2
Use security devices for authentication	12.3	34.0	4.9	3.4	21.4	54.5

Day to day responsibility for IT security varies by institution



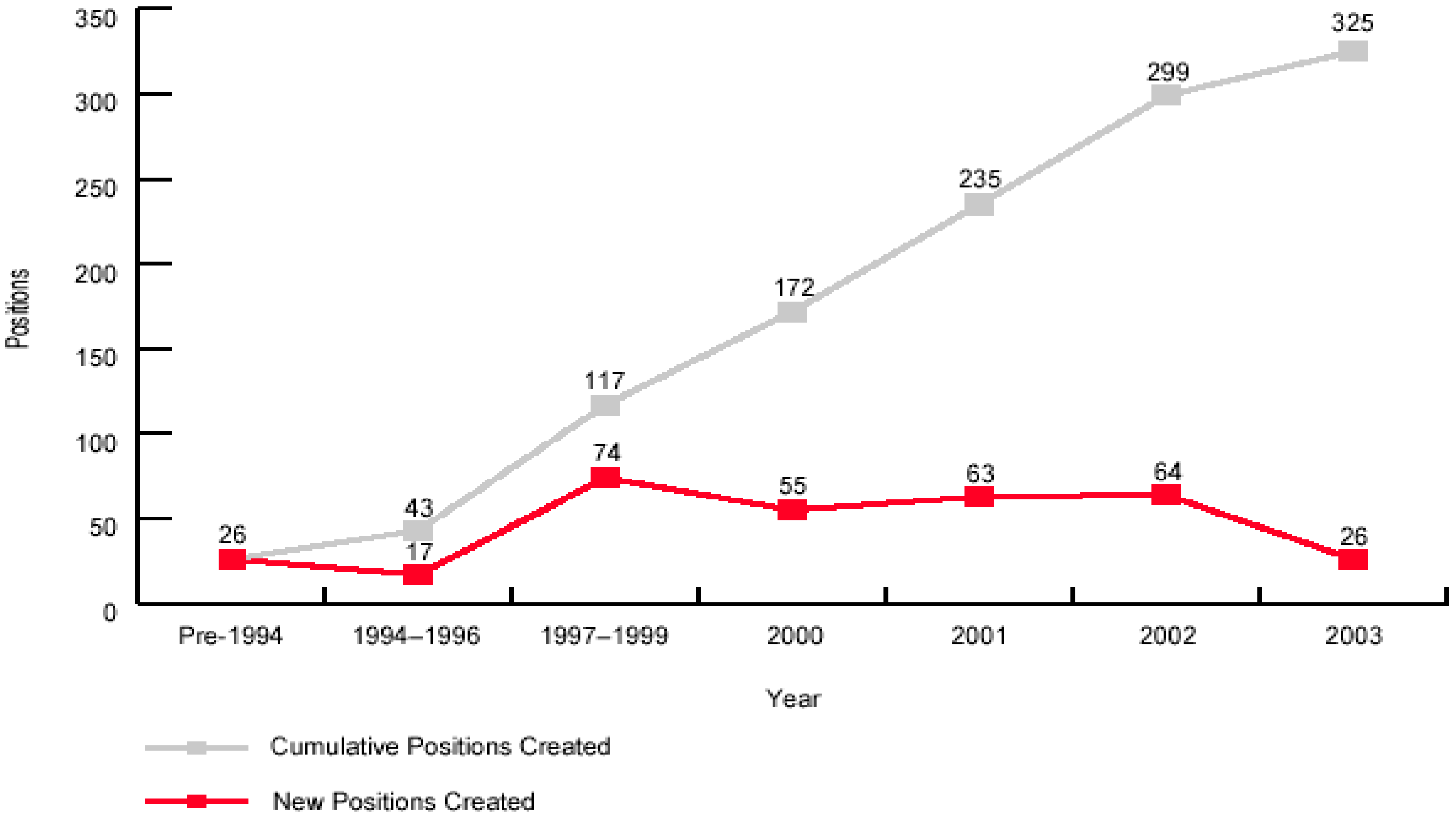
- 90% of Chief Security Officers work at Doctoral Extensive or Intensive institutions
- 12% of those with operational responsibility for IT security have an IT security certification

Staffing compliment and structure varies significantly



- 50% of respondents had at least one full time security staff member, with multi-person staffs most often reported at institutions with larger numbers of devices (10,000+) on their networks

Institutions continue to add IT security staff



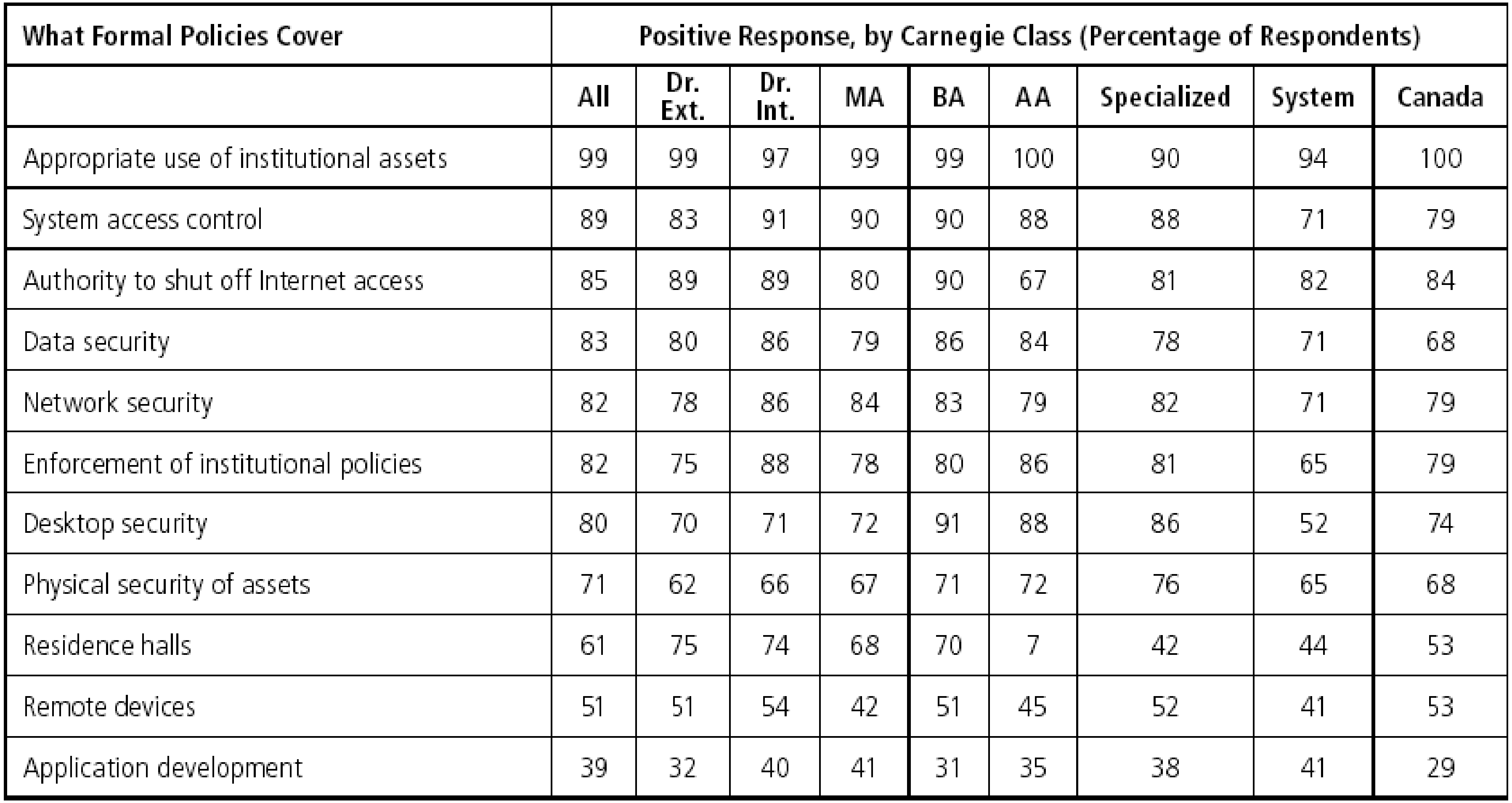
- 66% of respondents indicated that they did not expect the size of their IT security staff to change in the next two years. 25% expected to add one staff member, and 9% expected to add two or more

IT security budgets are expected to grow somewhat in the next year

	Percentage of Respondents			
Change in Expenditure	Staffing	Hardware / Software	Training	External Services
Significant Increase	2.6	9.0	5.4	2.5
Some Increase	25.6	38.7	37.0	19.2
About the Same	63.3	40.1	43.9	62.3
Some Decrease	7.6	10.6	11.1	12.3
Significant Decrease	9.0	1.7	2.6	3.7

- 55% of respondents spent between one and five percent of their IT budget on security. 14% reported spending six to ten percent, and 28% spent less than one percent.
- 44% of respondents disagreed or strongly disagreed with the statement that their institution provided the needed resources to address IT security issues. Only 28% agreed or strongly agreed.
- Interestingly, 75% of respondents agreed or strongly agreed that IT security was one of the top three issues facing their institution

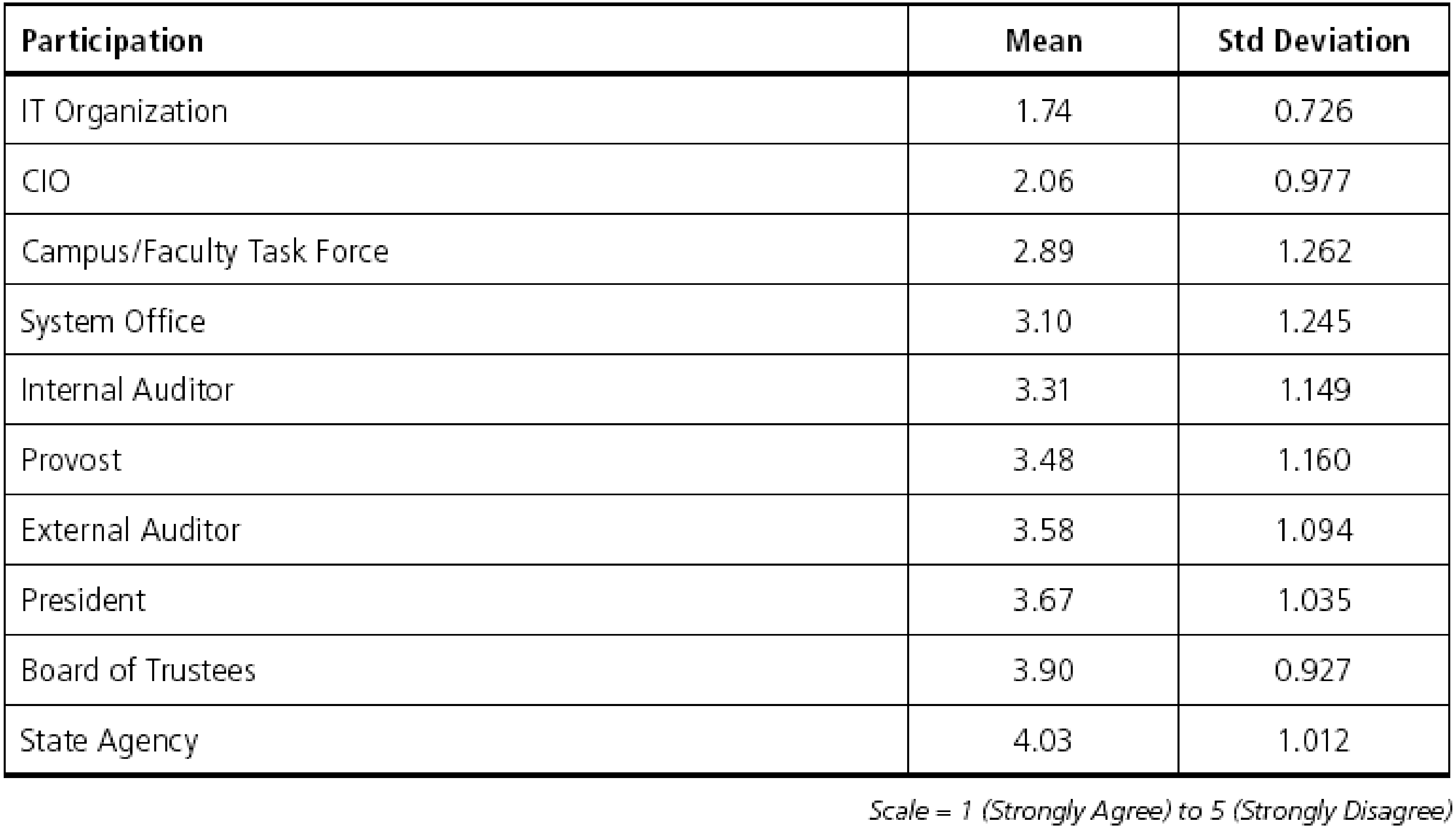
Institutions have created a range of IT security policies



What Formal Policies Cover	Positive Response, by Carnegie Class (Percentage of Respondents)								
	All	Dr. Ext.	Dr. Int.	MA	BA	AA	Specialized	System	Canada
Appropriate use of institutional assets	99	99	97	99	99	100	90	94	100
System access control	89	83	91	90	90	88	88	71	79
Authority to shut off Internet access	85	89	89	80	90	67	81	82	84
Data security	83	80	86	79	86	84	78	71	68
Network security	82	78	86	84	83	79	82	71	79
Enforcement of institutional policies	82	75	88	78	80	86	81	65	79
Desktop security	80	70	71	72	91	88	86	52	74
Physical security of assets	71	62	66	67	71	72	76	65	68
Residence halls	61	75	74	68	70	7	42	44	53
Remote devices	51	51	54	42	51	45	52	41	53
Application development	39	32	40	41	31	35	38	41	29

- 54% of respondents indicated formal IT security policies are in place at their institution, with only 8% having no policies of any kind

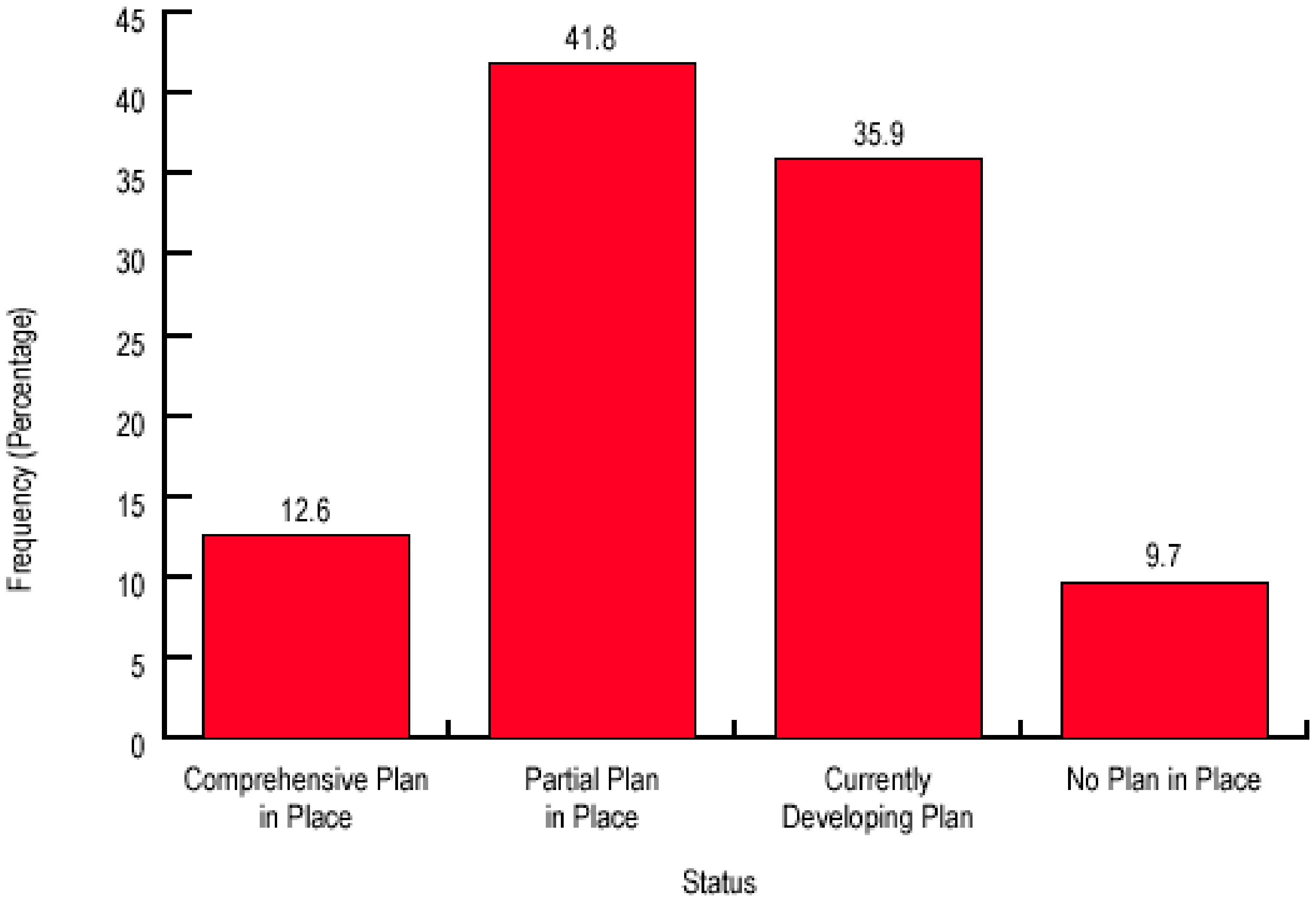
Leadership involvement in formulating IT security policy is often low



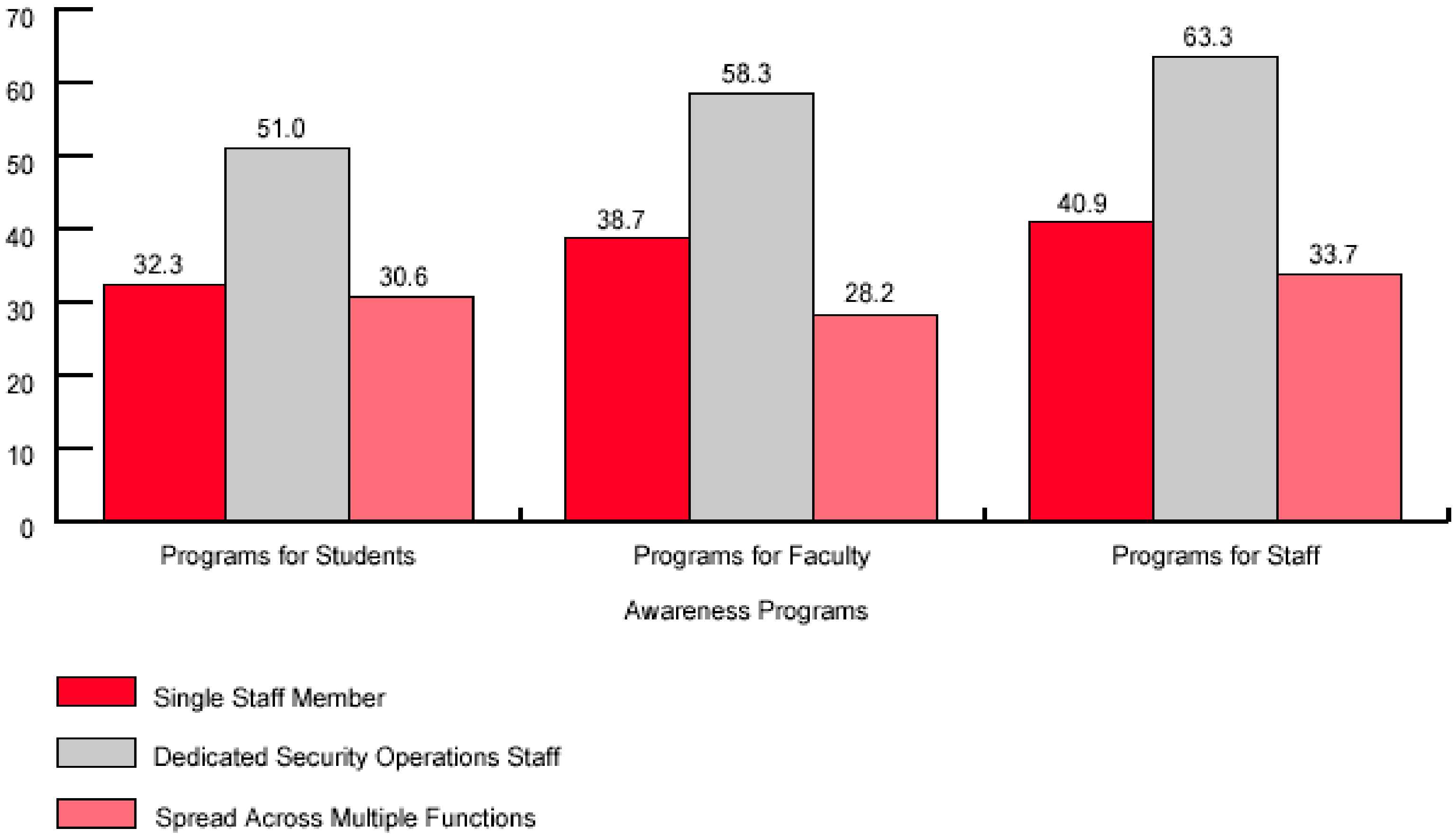
Participation	Mean	Std Deviation
IT Organization	1.74	0.726
CIO	2.06	0.977
Campus/Faculty Task Force	2.89	1.262
System Office	3.10	1.245
Internal Auditor	3.31	1.149
Provost	3.48	1.160
External Auditor	3.58	1.094
President	3.67	1.035
Board of Trustees	3.90	0.927
State Agency	4.03	1.012

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

Most respondents did not have comprehensive IT security plans in place

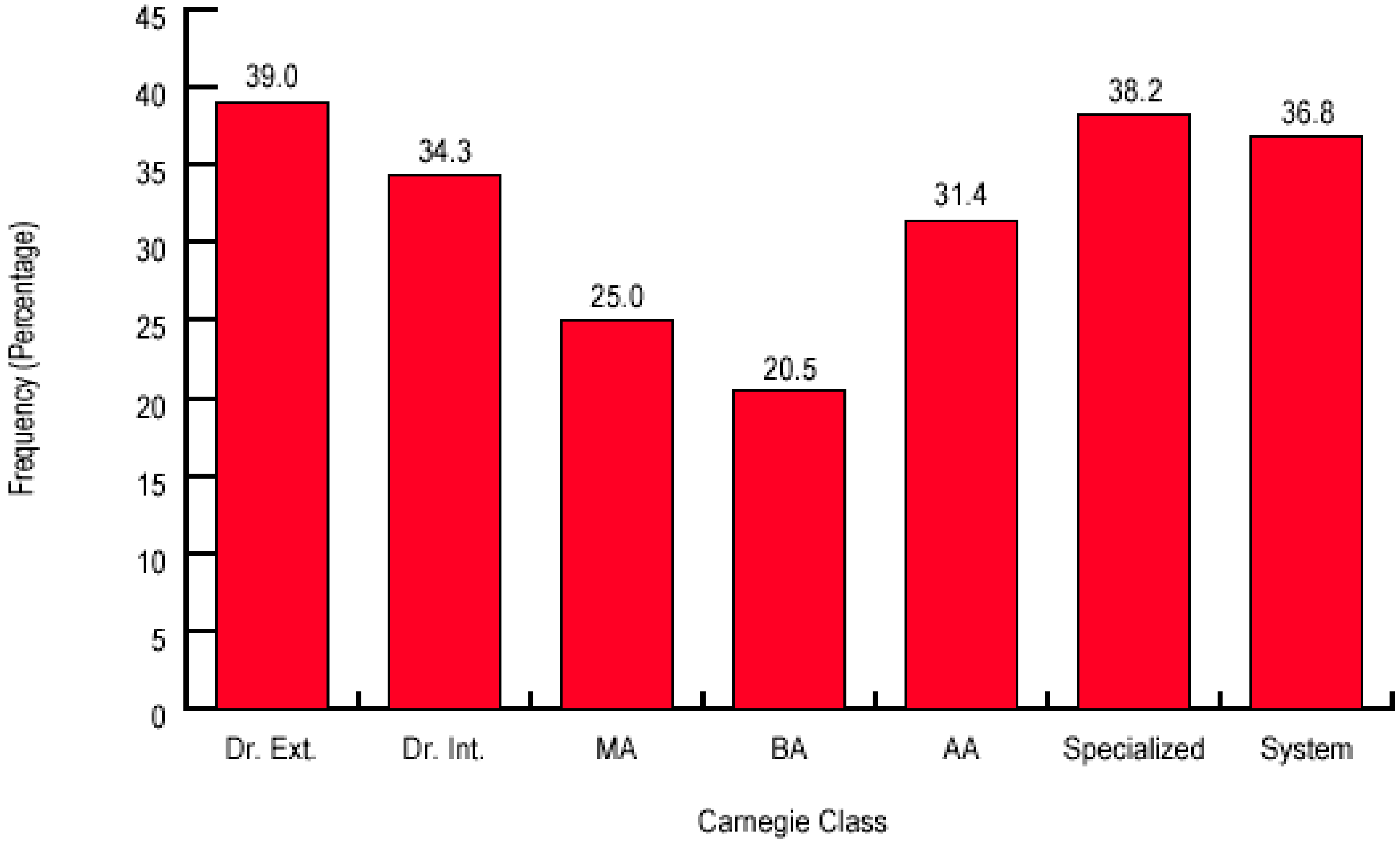


Awareness programs are most prevalent in organizations with a dedicated IT security team



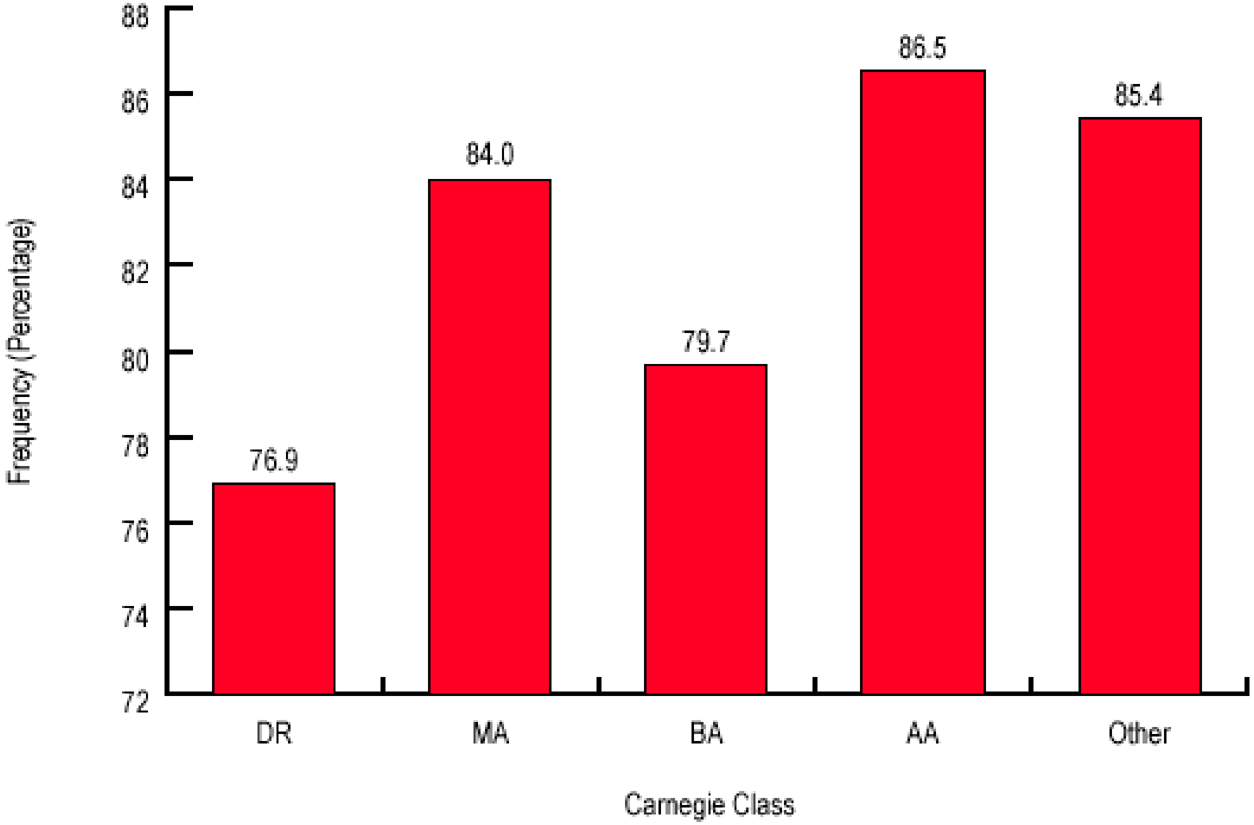
- Overall, under 40% of responding institutions had formal awareness programs in place

Larger institutions were more likely to have conducted a risk assessment, but the majority of respondents had not



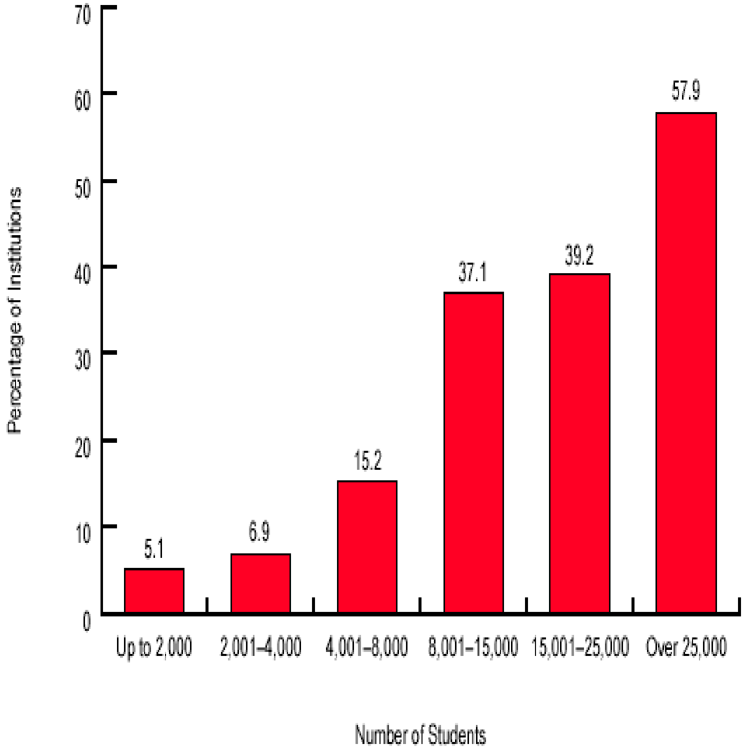
- Overall, under 30% of responding institutions had conducted a risk assessment

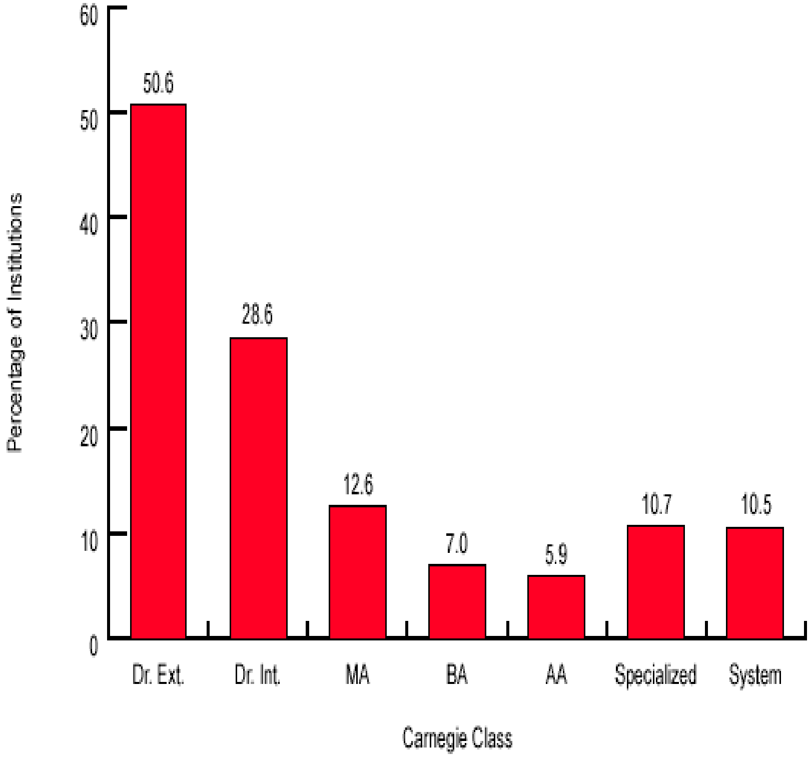
A large percentage of respondents required critical systems to be expeditiously patched or updated



- 62% require all campus owned computers on the network to have known security holes fixed.
- 59% indicated that they conducted regular scanning to detect known vulnerabilities on critical systems. 40% conducted such scanning on all systems connected to their networks

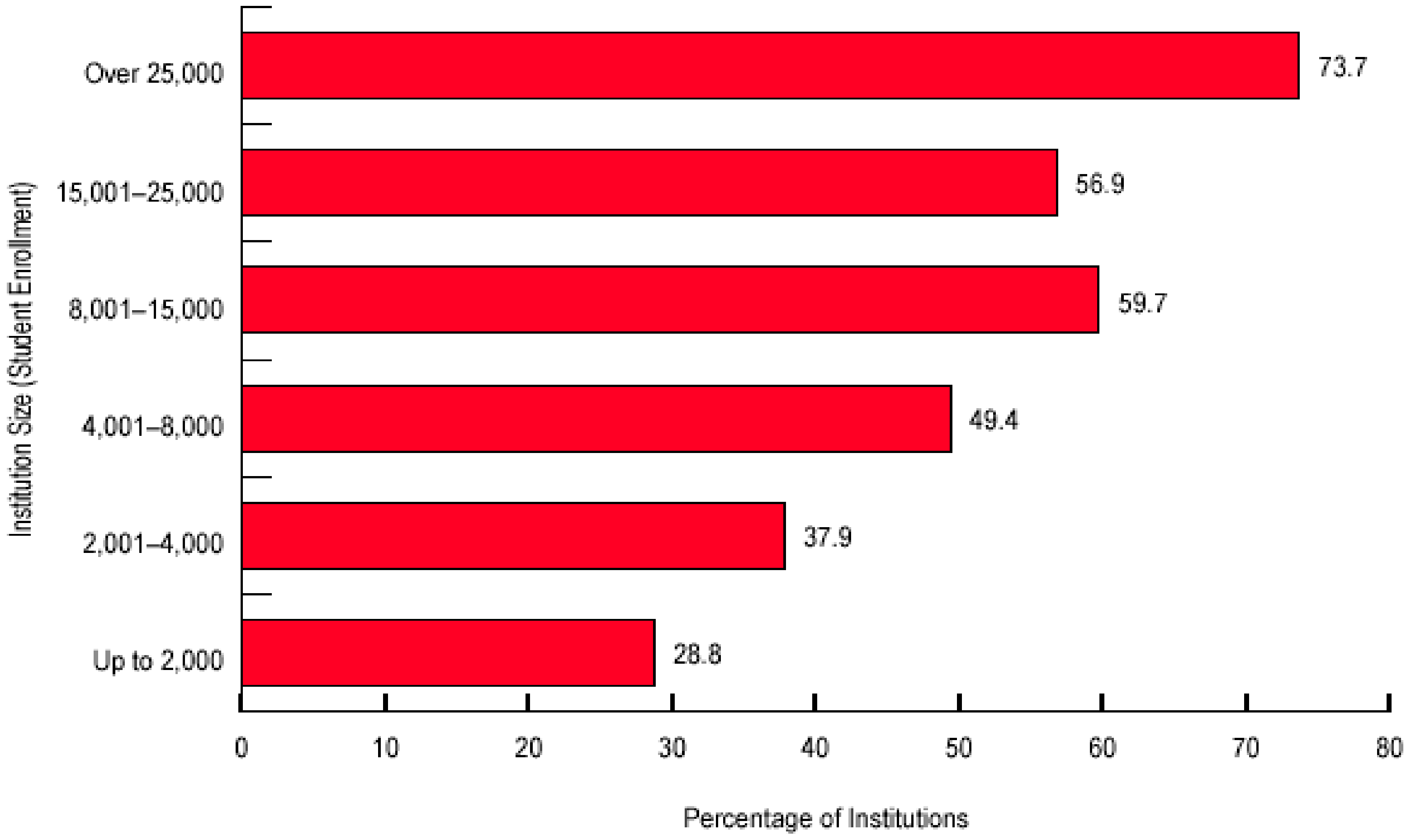
Larger institutions were more likely to have an incident reported in the press, but even the smallest had some



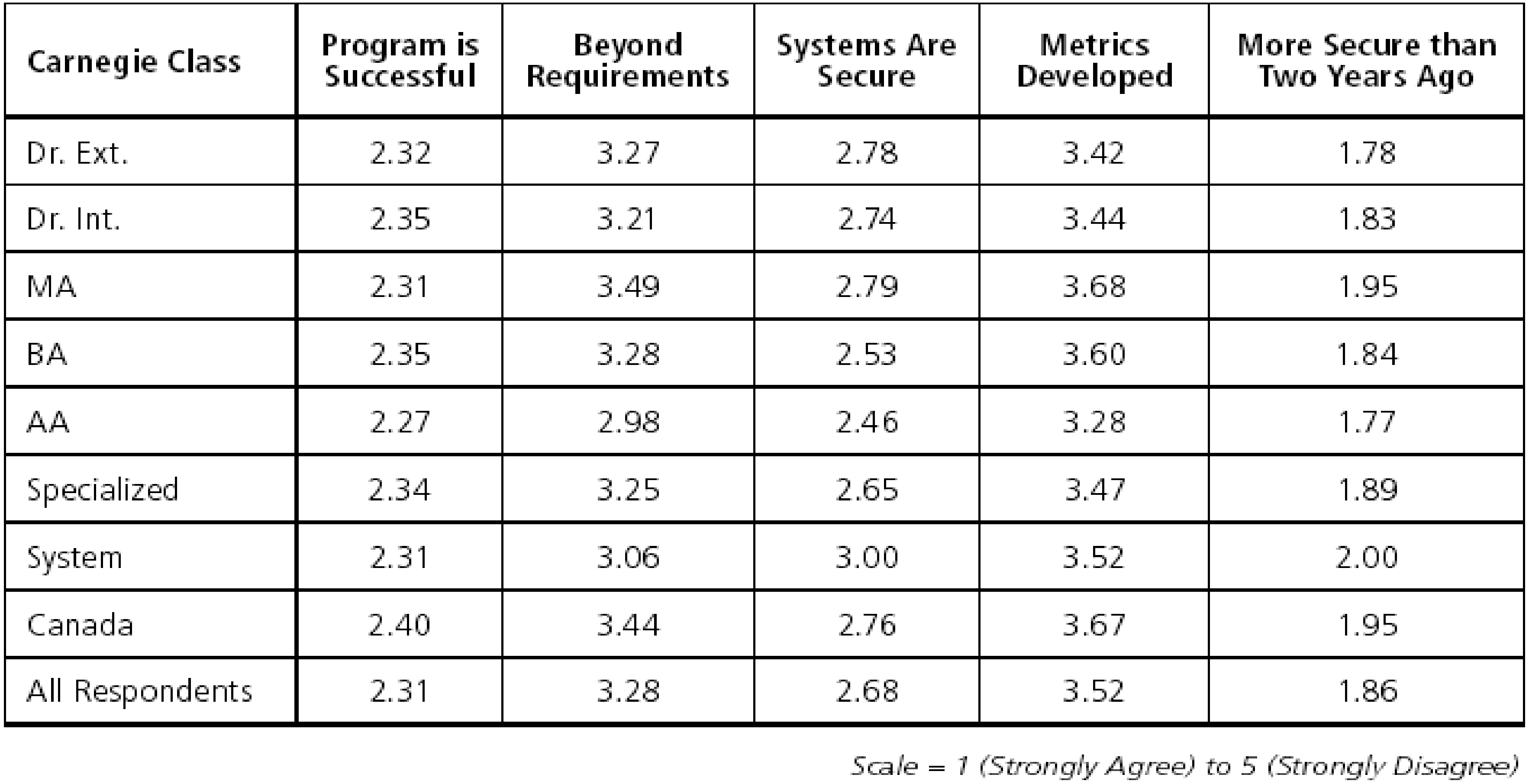


- 70% of reported incidents occurred at public institutions

Larger institutions were more likely to have formal incident handling procedures



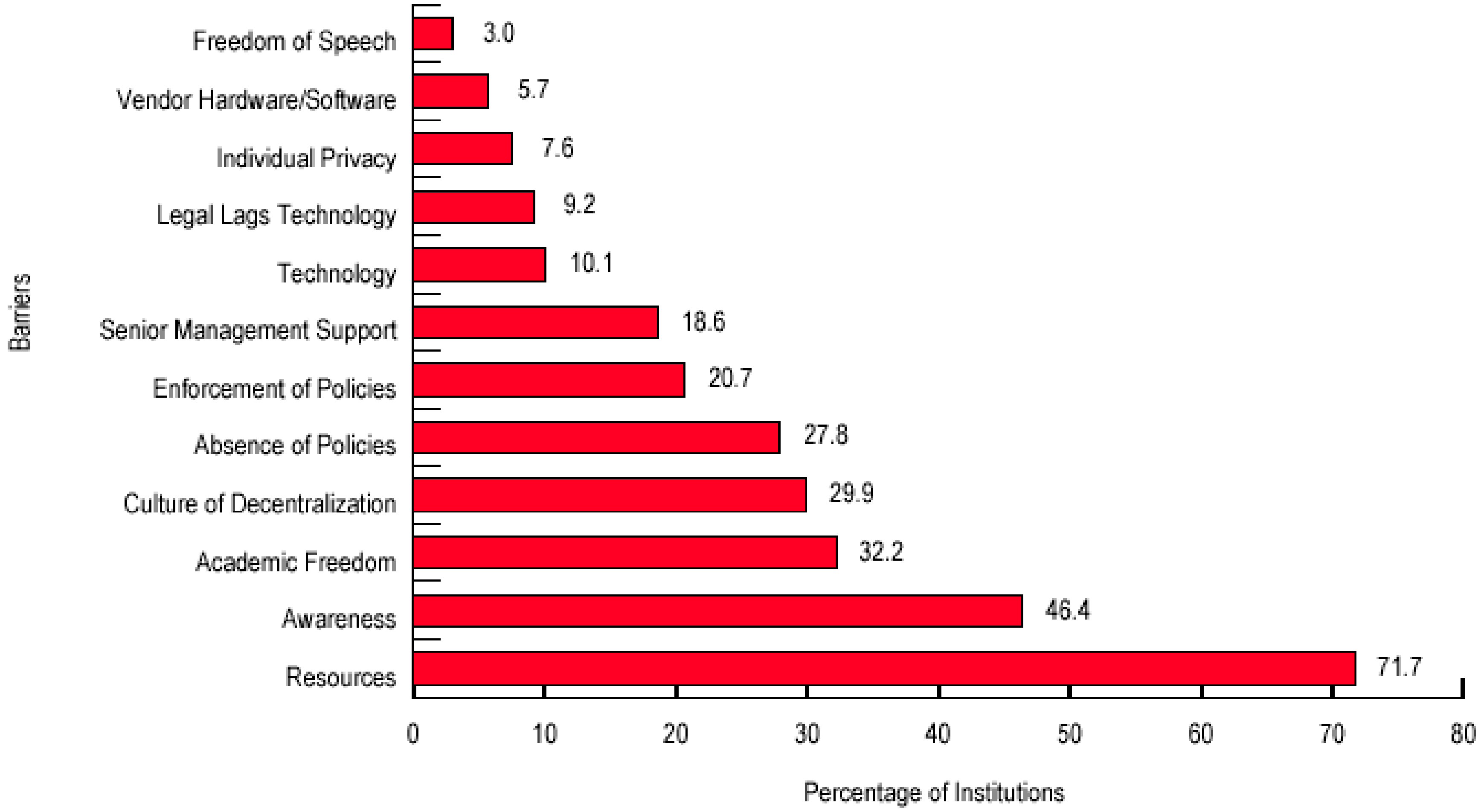
Respondents were mostly positive about the success of their IT security programs



Carnegie Class	Program is Successful	Beyond Requirements	Systems Are Secure	Metrics Developed	More Secure than Two Years Ago
Dr. Ext.	2.32	3.27	2.78	3.42	1.78
Dr. Int.	2.35	3.21	2.74	3.44	1.83
MA	2.31	3.49	2.79	3.68	1.95
BA	2.35	3.28	2.53	3.60	1.84
AA	2.27	2.98	2.46	3.28	1.77
Specialized	2.34	3.25	2.65	3.47	1.89
System	2.31	3.06	3.00	3.52	2.00
Canada	2.40	3.44	2.76	3.67	1.95
All Respondents	2.31	3.28	2.68	3.52	1.86

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

However, significant barriers are perceived



Lessons Learned

IT Security is not just about technology

- **Institutions that implemented the ‘softer’ aspects of IT security tended to feel significantly more secure**

IT security component	Program is Successful		More Secure Than Two Years Ago	
Dedicated staff vs. single staff member	2.00	2.47	1.56	1.94
Risk Assessment Yes vs. No	2.03	2.44	1.64	1.97
IT Security Plan Yes vs. No	2.20	2.54	1.76	2.18
Awareness Program Yes vs. No	2.00	2.50	1.66	1.98

Scale = 1 (Strongly Agree) to 5 (Strongly Disagree)

A number of other factors were identified as contributing to the success of IT security programs

- ***Engaged Leadership:*** Institutions whose president or provost were involved with IT policy development felt they were more successful
- ***Resource Availability*:** Institutions who felt they had allocated sufficient resources to IT security felt their programs were more successful
- ***Diligent Monitoring:*** A number of respondents felt that monitoring was critical to maintaining effective security
- ***Cultural Awareness:*** Security procedures that enable, rather than conflict with the academic mission / culture are more likely to succeed
- ***Proper Incentives:*** Users want to be secure, but won’t go far out of their way to get there. Making it easier for them helps.

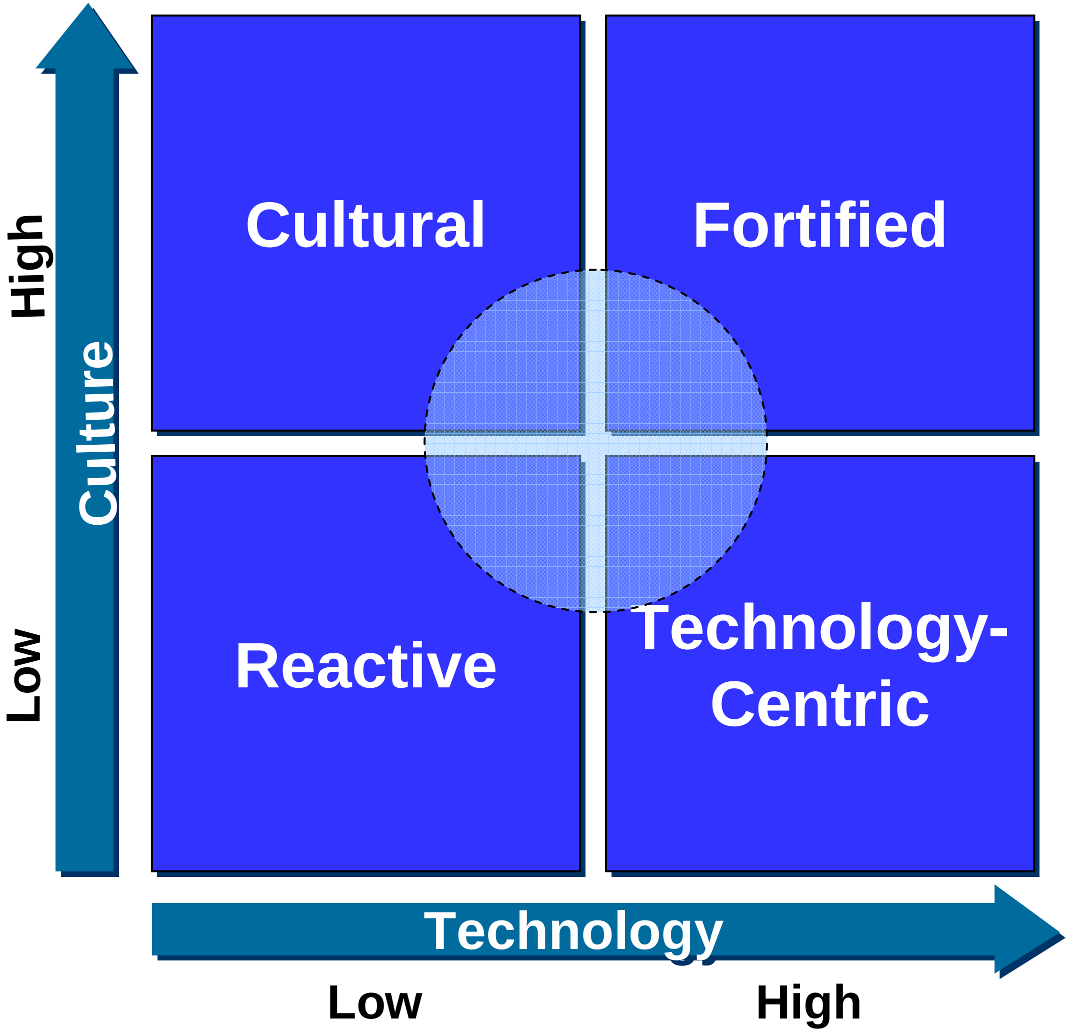
Two major IT security topics generated conflicting opinions

- **Firewalls**
  - Some institutions advocated host-based security, and did not use perimeter firewalls. They felt firewalls created many issues, did not work well in a research environment, and created a false sense of security.
  - Others argued that firewalls provided a strong first line of defense around their network, and made overall security management easier.
- **Policies**
  - At some institutions, strong, detailed IT security policies are in place, and are credited with helping to drive the success of IT security initiatives
  - At other institutions, IT security policies are general or informal, and are credited with giving the organization flexibility to respond on a case by case basis

Is IT security management inherently different in a higher education setting?

- **Our analysis found a number of common beliefs about the barriers to administering IT security in higher education to be manageable, if proper steps were taken. Some of these beliefs included:**
  - IT security inhibits academic freedom
  - IT security compromises personal privacy
  - IT security limits access to information
  - Openness and community outreach are at odds with IT security
  - A transient student body is difficult to manage
  - Faculty autonomy hinders uniform IT security standards
- **However, we did find some factors that did seem to be different in higher education, and impact the way IT security is managed. These included:**
  - Decentralization
  - Equipment diversity
  - Mission diversity
  - User diversity
  - Research requirements
  - Value of information assets

Overall, higher education seems to be pursuing a technology-centric approach to IT security



The Changing Environment

The IT security environment is rapidly changing, and may bring significant change

- **New technologies:** Tools available to manage IT security are rapidly becoming more available and more capable, as are the tools available to hackers
- **Legal environment:** The legal environment surrounding IT security is becoming more complex, presenting both challenges and opportunities
- **Changing nature of threats:** Automated attacks are replacing individual hackers as the most likely cause of a security breach
- **Demands for increased accountability:** Institutions will come under increased pressure from their constituents to provide robust IT security, as its profile rises
- **Centralization and standardization:** The changing nature of threats, and the increasing sophistication needed to combat them may prompt a move to more centralized and standardized management of security at large institutions
- **Sharing the burden**: Many institutions, particularly smaller ones, may seek assistance from consortia or vendors in managing the increasing burden of IT security management

Questions and comments

Robert Kvavik: kvavik@umn.edu