

**EDUCAUSE/Internet2 Computer and Network Security Task Force
2008–2009 Strategic Plan**

Safeguarding Our IT Assets, Protecting Our Community's Privacy





Established by EDUCAUSE and Internet2 in July 2000, the EDUCAUSE/Internet2 Computer and Network Security Task Force works to improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures. For more information, visit www.educause.edu/security.

EDUCAUSE/Internet2 Computer and Network Security Task Force 2008–2009 Strategic Plan

Safeguarding Our IT Assets, Protecting Our Community's Privacy

Introduction

The EDUCAUSE/Internet2 Computer and Network Security Task Force (STF) provides a focal point for the academic community to join together to strengthen the ability of the higher education sector to respond to growing threats to information security and to protect the privacy of our community members. This strategic plan is intended to set forth a vision for the higher education community and provide a concise roadmap to guide the efforts of the STF. This roadmap emphasizes continuous and evolutionary community investment in converting our understanding of risks and issues into solutions based on effective practices, as well as the urgent need to build the national capability across the higher education sector to respond quickly and effectively as a community to new threats and vulnerabilities.

History

The STF was established in July 2000 to address concerns that college and university networks were being used to launch distributed denial-of-service (DDoS) attacks against computer systems owned by the government and the private sector. Although initially formed to minimize the adverse impacts of such attacks, it was quickly apparent that it was in higher education's best interest to improve the security of campus computer systems in order to protect the higher education sector's interests as well.

Beginning in 2002, the STF was asked to engage with the White House and federal agencies in the development of a coordinated national effort to improve cybersecurity. As part of that effort, the higher education community was asked to respond to the following questions:

- How can academic freedom of inquiry be maintained while at the same time preventing the large scale computing power of universities from being hijacked for denial of service attacks and other malicious activity directed at other sites?
- What functions on a university system require high levels of IT security (e.g., medical records, research trials, patents), and how is that best achieved within the context of an academic setting?
- How can universities best organize to address the IT security questions they face in common? Should best practices or standards be agreed to on a national level? Should there be a mechanism for information sharing on threats and vulnerabilities among university CIOs and systems administrators?

The STF received a grant from the National Science Foundation to seek to answer these questions and to explore the needs of the community. In 2003, the STF prepared *The Higher Education Contribution to the National Strategy to Secure Cyberspace*. This document encouraged colleges and universities to secure their cybersystems by establishing some or all of the following as appropriate:

- One or more Information Sharing and Analysis Centers (ISACs) to deal with cyberattacks and vulnerabilities
- An on-call point-of-contact to Internet service providers and law enforcement officials in the event that the school's IT systems are discovered to be launching cyberattacks
- Model guidelines empowering CIOs to address cybersecurity
- One or more sets of best practices for IT security
- Model user awareness programs and materials

Academia is recognized as an important resource in our national efforts to improve cybersecurity. Through its core mission of *teaching and learning*, it is the main source of our future leaders, innovators, and technical workforce. Through *research*, it is the basic source of much of our new knowledge and subsequent technologies. As complex institutions, colleges and universities operate some of the world's largest collections of computers and high-speed networks. The STF has become the leader in helping address the challenges confronting colleges and universities as owners and operators of cybersystems. The STF also partners with other academic organizations that provide cybersecurity leadership in the areas of curriculum, career development, software assurance, training, and research and development.

The STF has become the key organization for helping institutions of higher education improve their IT security posture primarily through its efforts to raise the visibility of IT security issues among campus leaders and to organize the IT security community. The STF began the Security Professionals Conference in 2003 as a venue to annually bring together security practitioners from across the higher education landscape for professional development and face-to-face networking. The STF seeks to represent all of higher education and has received the support of the six presidential associations: the American Council on Education, the American Association of Community Colleges, the Association of American Universities, the American Association of State Colleges and Universities, the National Association of Independent Colleges and Universities, and the National Association of State Universities and Land-Grant Colleges.

The STF is also recognized as the sector coordinating council for higher education with respect to the protection of cyber assets and participates with the U.S. Department of Homeland Security, the U.S. Department of Education, and other partners in the implementation of the National Infrastructure Protection Plan. The Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) at Indiana University provides a trusted information-sharing network for the dissemination of critical threats and warnings and exchanges information, as appropriate, with other sector ISACs.

Host Organizations' Strategic Plans

EDUCAUSE and Internet2 worked together to form the STF. Recognizing the complementary nature of the two organizations, the STF combines the energy and expertise of the two organizations' constituencies and coordinates activities between the organizations' staffs. Each organization recently undertook a strategic planning process. The results, summarized below, were used to inform the future directions of the STF.

EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. The current membership comprises more than 2,200 colleges, universities, and educational organizations, including 250 corporations, with 17,000 active members.

EDUCAUSE aspires to be known in three years for its high value to members, leadership, engagement, partnerships, coherence, and continuous innovation. EDUCAUSE will be responsive and member-focused, will proactively surface emergency trends and synthesize information, will take a leadership role on important community issues, will help members be change agents on campus, and will become a more agile and focused organization. It has identified four focus areas: teaching and learning, managing the enterprise, e-research and e-scholarship, and the evolving role of IT and leadership. Privacy and security, while critical issues for "managing the enterprise," also touch upon the other focus areas. EDUCAUSE will address each focus area through some or all of the following activities: knowledge creation and dissemination, collaboration and community, policy analysis and advocacy, career and leadership development, and experimentation.

Internet2 is the foremost U.S. advanced networking consortium. Led by the research and education community since 1996, Internet2 promotes the missions of its members by providing both leading-edge network capabilities and unique partnership opportunities that together facilitate the development, deployment, and use of revolutionary Internet technologies. Internet2 brings the U.S. research and academic communities together with technology leaders from industry, government, and the international community to undertake collaborative efforts that have a fundamental impact on tomorrow's Internet.

Internet2 aspires to promote new approaches to collaboration, security, and privacy services that enable faculty, staff, and students at every member institution to use their institutional credentials to securely access local, national, and international academic resources. It will also strive to develop and promote cost-effective methodologies, standards, and best practices for security and end-to-end application performance. Internet2 also seeks to leverage its position of national and international leadership of programs in middleware for identity services and security by advancing development efforts and aggressively promoting deployment throughout the academic community. It will work with EDUCAUSE, government agencies, and other domestic and international partners to identify and address the security challenges unique to advanced networks and higher education.

Vision

The STF will be recognized as playing an essential leadership role in helping transform our academic institutions, large and small, to safeguard the security of information systems at the highest levels and to protect the privacy of our community and those they serve, through strong commitment and innovation on the part of our community and focused partnerships with the private sector and government.

Mission

The STF works to improve information security and privacy across the higher education sector by actively developing and promoting effective practices and solutions for the protection of critical IT assets and infrastructures, both through the work of its community members and through focused partnerships with other government, industry, and academic organizations.

Themes and Goals for 2008–2009

Although computer and network security has been the STF's focus of attention during the past few years, the STF has adopted the theme of "Safeguarding Our IT Assets, Protecting Our Community's Privacy" for 2008–2009. The STF strategic planning process aims to anticipate higher education security issues, enabling campuses to forge joint efforts and solutions and recognizing that security challenges continue to evolve in our digital information world. Consequently, the following goals and associated actions have been identified for 2008–2009 to help focus working group priorities in the near term (12–18 months):

1. Obtain Executive Commitment and Action

Background

College and university information security officers repeatedly report that one of their greatest challenges is gaining executive support for their information security program. While significant or high-profile data privacy incidents have forced some campus executives to pay attention and devote resources to improving privacy and security, there does not appear to be the ongoing commitment necessary to sustain improvements over the long term. Additionally, it is sometimes difficult for information security to be considered a priority for campus leaders due to competing demands for their time and attention. Therefore, the STF should surface examples of successful efforts to obtain executive commitment and action and seek methods to help other institutions raise the profile of information security among campus executives and governing boards.

Actions

- 1.1 Develop and promote resources that will assist institutions of higher education to incorporate information security into its enterprise governance efforts.
- 1.2 Build or assemble a set of core resources with key messages for campus executives.
- 1.3 Establish an outreach plan to reach other professional associations with core content designed for campus executives.
- 1.4 Develop information security metrics for use with campus executives.
- 1.5 Promote a risk management framework for protecting cyber assets.
- 1.6 Identify and promote critical success factors that support creating and sustaining effective information security programs.

2. Manage Data to Enhance Privacy and Security Protections

Background

Although computer and network security continue to be significant concerns of the STF, it is apparent that our focus has shifted in the recent past to focus on data privacy and security. The emphasis on data protection also forces us to think about information in both paper as well as electronic form, despite the historical connections of EDUCAUSE and Internet2 to the community of IT practitioners. It also necessitates the engagement of data stewards and others who are responsible for the privacy and security of data. It is imperative that the STF redouble its efforts to focus on ways that we can better manage data given the high number of incidents of unauthorized data disclosures at colleges and universities.

Actions

- 2.1 Expand the collection of resources that support the Confidential Data Handling Blueprint and distribute broadly.
- 2.2 Develop and promote the Data Classification Toolkit to assist institutions in their efforts to categorize data and assign responsibility.
- 2.3 Create a national cybersecurity awareness campaign to improve information security and privacy across the higher education sector.
- 2.4 Establish and promote guidelines for data and media sanitization, including anonymization, to address disposal or disposition of technology assets.
- 2.5 Research and communicate the privacy and security implications of outsourcing data handling to establish guidance and recommended practices for the community.
- 2.6 Develop mechanisms to help the community address related issues of electronic records management, e-discovery, data retention, and so forth.

3. Develop and Promote Effective Practices and Solutions

Background

One of the cornerstones of the STF has been the facilitation of sharing of effective practices and solutions among members of the community. The STF working groups have also been productive contributors of content, developing new resources or tools when they do not already exist. The *Effective IT Security Practices Guide* is in its second edition and is being compiled in a wiki format to permit a more dynamic environment for ongoing contributions from the community. However, we need to more aggressively pursue a set of strategies and tactics that will make this resource usable by the community it is intended to serve. We have also effectively engaged vendors as active participants in the annual security conference, but we have been less successful in creating ongoing mechanisms for engagement in areas of mutual interest and concern.

Actions

- 3.1 Create and execute a promotional plan to draw attention to the *Effective IT Security Practices Guide* as the key STF resource that provides practical approaches for IT security in higher education.
- 3.2 Create a framework for categorizing and organizing the guide that leverages existing frameworks and standards.
- 3.3 Develop a structure for coordination of the guide and assign roles and responsibilities.
- 3.4 Coordinate mechanisms for regularly polling the community to identify areas in which effective practices are needed.
- 3.5 Establish processes for the collection or creation of effective practices and solutions.
- 3.6 Engage industry partners in the promotion of effective practices and solutions that leverage commercial products and services.
- 3.7 Promote a set of security metrics that will allow institutions to measure progress within their institution and compare successes across institutions.

4. Explore New Tools and Technologies

Background

It is expected that information security threats and vulnerabilities will continue to change. Consequently, the development of new solutions as well as refinement to current approaches will be required. The STF can help guide the development of community-sourced solutions as well as inform the direction of commercial products and services. Security considerations are also critical to efforts to redesign the Internet and the development of cyberinfrastructure in support of e-science. Additionally, the STF must be positioned to collaborate with government agencies and other domestic and international partners to identify and address the security challenges unique to advanced networks and higher education.

Actions

- 4.1 Create mechanisms for assessing community needs to address new or persistent challenges or trends that require us to rethink conventional approaches to information security.
 - 4.2 Engage industry partners in the exploration and development of next - generation solutions.
 - 4.3 Identify and participate in the cybersecurity R&D forums established by other organizations to provide community input and bring back information.
 - 4.4 Establish model frameworks for security architecture that support privacy and security goals of institutions of higher education.
 - 4.5 Strengthen collaboration with middleware and identity management initiatives of EDUCAUSE, Internet2, other organizations, and international partners.
5. Establish and Promote Information-Sharing Mechanisms

Background

The STF can take considerable pride in the establishment of a community of security professionals within higher education. The STF has established several venues for collaboration and must continue to refine our information-sharing mechanisms to ensure that they are complementary and not duplicative in purpose or operation. We will need to continue to promote existing mechanisms as the community continues to grow and as turnover occurs at colleges and universities. We must also be open to new opportunities and changing requirements to address community needs, including the sharing of sensitive information.

Actions

- 5.1 Establish mechanisms for identifying and orienting new security professionals to the community of peers and resources available.
- 5.2 Promote and leverage the EDUCAUSE Security Discussion Group as a communication vehicle for the higher education community.
- 5.3 Explore other effective methods of communicating information to the community, including blogs, RSS feeds, websites, and other technologies.
- 5.4 Finalize new membership model for the REN-ISAC and develop an active plan to sustain membership and recruit new members.
- 5.5 Enhance the annual security conference experience to include more formal and informal means for face-to-face networking.
- 5.6 Establish partnerships with other information-sharing organizations including US-CERT, FIRST, ISAC Council, InfraGard, Electronic Crimes Task Forces, and others.

Conclusion

As members of the higher education community, the STF recognizes the significant challenges in improving IT security at colleges and universities. While the urgency has in the past focused on reducing institutional risk by protecting IT assets, our community has come to recognize the importance of protecting the privacy of institutional information, as well as that of other stakeholders (including alumni, donors, guests, and others) who come into contact with our institutions. Our goals and strategies are intended to help direct assistance within the community in ways that are both cost-effective and timely. While the scope of information security and assurance is broad, an agile strategic plan, such as this one, helps the community to respond quickly to the ever-changing risks that develop in this volatile and exciting arena.