

EDUCAUSE Center for Applied Research

Research Bulletin

Volume 2006, Issue 24

December 5, 2006

Local IT Security for Colleges, Schools, and Departments: A Higher Education Perspective

Derek Spransy, Emory University



The recently published 2006 ECAR study on information technology (IT) security in higher education reports that there has been a sea change in college and university security practices since 2003. In the face of security threats and breaches, our institutions have made significant strides in the protection of data and institutional infrastructure investments, and enterprise-wide security strategies are now the norm rather than the exception. In the decentralized culture of many collegiate environments, individual schools, departments, and laboratories continue to control a portion of their IT assets, and this fact hampers the institution from implementing across-the-board security solutions. Instead of being in a position to automatically push new security patches or virus protection software to all devices on the network, campus IT security officers must educate and persuade the departmental IT administrators and the user community to practice “safe” computing (Kvavik, 2006).

As a result of this decentralized structure, central IT services can only be so effective against the myriad threats that university computer networks and systems face. Some of the primary threats to a network reside at the network end points, and a portion of the responsibility for securing the university network ultimately falls to individual colleges, schools, departments, and business units. In fact, it is common for decentralized units to “augment” the security functions of central IT (Pirani, 2004). These entities must take the initiative in developing strategies to secure their own environments. This task is often best accomplished when strategies are developed with the collaboration and input of central IT, and with the strategic goals of the school and institution in mind.

The IT structure at Emory University is a decentralized model. Many schools and business units at Emory have their own local support personnel, services, and policies and procedures. This bulletin discusses some of the lessons learned by one such school, Emory College, Faculty of Arts and Sciences—known as Emory College—in developing its security strategy, as well as what other schools grappling with security should consider when implementing their own local security strategies. Research is drawn from the experiences of Emory College, along with interviews of IT lead personnel from five of Emory University’s other graduate and undergraduate schools: the School of Law, the School of Nursing, the School of Medicine, the School of Public Health, and the School of Business.

Highlights of a Local IT Security Strategy

The character of security incidents has shifted over the last several years from events that affect a relatively small group or single system to events that affect thousands of systems or individuals. It is no longer sufficient to mandate tight controls on a small set of users or IT professionals to create an effective security blanket. (Boes, Cramer, Dean, Hanson, & McKenna, 2006, p. 4)

The first step that must be taken when developing a security strategy is to define the scope of the strategy itself. This information forms the framework of a security policy and guides the strategy throughout its development.

Define What Must Be Secured

Defining what must be secured, in terms of data and infrastructure, helps identify the technologies that must be implemented. Start by thinking about what will need to be protected. This may include student, faculty, and staff personal information, research data, desktop computers, departmental servers, network components, and so forth. Is the strategy only concerned with securing desktop computers owned by the school, or must the strategy also include servers, laptops, smartphones, and student computers that may be owned by individual faculty, staff, and students? How much of the computing environment is actually managed by the school's IT staff?

To make these boundaries clear, it's important to understand where the responsibilities of security begin and end, and in what ways the individual school's responsibilities intersect with those of central IT. Table 1 provides brief examples of the security services and responsibilities of Emory's central IT Academic and Administrative Information Technology Division (AAIT) and those of Emory College.

Table 1: Security Services Provided by Unit

	AAIT (Central IT)	Emory College
<i>Services</i>	Campus firewall DMZ VPN access Identity management (LDAP, Active Directory) Security certificates	Antivirus Patch management Desktop firewalls Security standards and configurations
<i>Responsibilities</i>	Border network Administrative data (PeopleSoft, financial systems) E-mail Web hosting Account security Incident response at university level Security awareness at university level Enterprise security strategy	Desktop and laptop computers Departmental servers Local IT services Research data and intellectual property Incident response at local level Security awareness at local level Local security strategy

Define the Threats

Once it is clear which assets should be protected, work can begin on defining and understanding the threats posed to them. Arguably, student records, intellectual property, and research data are the lifeblood of many institutions. While some of these

assets may fall under the scope of central IT security, it is not uncommon to find this information stored on unsecured end-point devices. Therefore, the responsibility of securing that data lies at the unit level. The loss of this information could have a potentially devastating impact on the institution and the research and academic processes. Open access policies and the absence of central control have historically made higher education networks and computers havens for malicious individuals and activity, which can result in unwanted information exposure, loss, or compromise. One need only look at recent security breaches within institutions of higher education to understand the potential risks. Once these threats are clearly understood, a strategic plan can be put into place to begin identifying and protecting data and assets.

Know Your Environment

The environment of a school, both technological and cultural, has one of the most fundamental impacts on IT security strategy development. A security strategy must not only provide security for data and assets, but it must also support the needs and the mission of faculty, staff, students, and the school itself. Emory College faculty members are involved in research disciplines that cover a broad spectrum. An art history professor might be researching stained glass windows of medieval France, while a chemist might be working on molecular imaging. Each of these faculty members has unique computing needs, yet their need for secure computing resources to accomplish their research and teaching goals is similar.

Understanding the needs of your users is vital when developing a comprehensive security strategy. Differing academic disciplines will produce differing computing needs. The chemist might have requirements for remote access that the art historian does not. The art historian may only require the resources of her desktop computer, whereas the chemist may have the need for a large computing cluster. Determining a method to provide secure computing resources to all disciplines is an essential ingredient to developing a successful security strategy. Ernesto Ince, Manager of Information Technology for Emory's Woodruff School of Nursing, noted that IT security "is easier in an environment where everyone is working on mostly the same kind of research than [it is] in a school where there are many different types of users and researchers."

One of Emory College's primary IT security strategies is to deliver a transparent, secure environment so that users can work seamlessly and safely. For the sake of consistency and ease of management, we have attempted to set and maintain a baseline of security standards for every computer under our scope of control. There are certainly exceptions, but we've found that this method works well for us in an environment with limited staffing.

This is not necessarily the best approach for every organization, and different levels of security may be necessary for different schools and departments within a school. Grant requirements, as well as regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA), will also play a major role in security strategy development. A medical school likely has to abide by far more third-party regulations than does a business or law school. Knowing your environment goes a long way in determining which strategy will fit the needs of your faculty, staff, and students.

An often repeated axiom about security is that as a system becomes more secure, its usability decreases. In many respects this is true. Consider the usability requirements of your faculty and staff. It may be decided that users shouldn't have the ability to install software, or that remote access capabilities should be removed. Secure configurations and policies may be seen by some as imposing restrictions on academic freedom. Given the culture of educational environments, this is a valid and perfectly understandable concern. Institutes of higher education pride themselves on having an open, collaborative atmosphere, and a security strategy should reflect and respect that orientation as much as possible. However, for the sake of security some policies and guidelines, such as those mentioned above, will have to be set forth.

Marc Overcash, CIO for Emory's Rollins School of Public Health, observed that "Policies are written at a point in time framed within a set of assumptions and expectations. As new business practices emerge and these assumptions and expectations are tested, these policies can interfere with the daily activities of the institution. It is the responsibility of our IT department to partner with the faculty, staff, and students to continuously evaluate and tune these policies to enable work to be done, but done securely based on the acceptable risk of the institution." It's important to realize that each school is only one part of the greater ecosystem of the institution. As Andrea Georgalis, Senior IT Project Manager for Emory's School of Medicine, stated, "Some groups will not implement security, and our separateness makes it difficult for each school to communicate and coordinate, leading to a more 'siloe'd' environment."

Get Administrative Buy-in

It is important that the local school or department administration understands not only the need for security but also its purpose and goals. Having executive support will make the implementation of a security strategy much easier. IT leaders should also take the opportunity to educate members of the school's administration on potential security concerns, risks, and exposures.

Ben Chapman, Assistant Dean for Information Technology at Emory's School of Law, said, "Without a [security] policy in place, you don't have the ammunition that you need in order to receive support from higher levels in the organization when it comes to security matters."

Work with Central IT

Although IT groups typically have the depth and breath of knowledge necessary to ensure proper IT security, even the best-resourced office is unlikely to be positioned to manage security for every application and system on campus, especially those run or administered by other departments and business units.

Ultimately, IT security depends on collaborative efforts among centralized and local resources. (Boes et al., 2006, p. 4)

It is common within an institution for local support providers in different IT units to "go it alone" when planning a security strategy or providing services to their client base. There

are numerous reasons for this practice, and many are perfectly valid. Central IT may not be able to meet the requirements of each individual school. Indeed, school- and department-level IT leads across Emory echoed the feeling that, in a decentralized environment, they feel better suited to quickly adapt and change to the growing IT security needs of their users. Georgalis said, “A decentralized environment allows each unit the flexibility to implement policies and procedures that best suit their environment. The College and the School of Medicine have different security needs, and we can meet the needs of our schools when we implement our own security plans.”

Despite this, central IT can be an invaluable resource when developing a security strategy. While individual schools may be more nimble than central IT, the latter should set the overall course for security strategy and direction. It can provide information on enterprise-level security services and policies. Not only can central IT act as an advisor during the planning phase, but it can also assist in making sure that the security strategy for the school or department supports the strategic IT goals and direction of the institution.

While central IT can be a great security resource for individual schools, the reverse is also true. A number of security needs and issues arise at the local unit level. It has been the experience of Emory College that the needs of users at the unit level drive much of the technological innovation and change within the institution. New and emerging technologies such as mobile computing create security challenges that must be addressed. Overcash stated, “You have to provide security controls that allow [for] research and collaboration. Faculty members want to bring in new and emerging technologies. The question then becomes, how do you bring that into our environment without introducing additional risk?”

Individual schools can communicate these new and emerging needs to central IT in order to collectively develop solutions. By doing so, schools are collaborating and actively participating with central IT not only to secure university resources but also to influence and guide the security strategy of the university itself.

Leverage Existing Resources

When implementing a security strategy it can be of great benefit not to reinvent the wheel by providing redundant security services, especially with limited staffing and budgets. Central IT may offer an array of security services that can benefit schools both directly and indirectly. Emory is fortunate enough to have a wide range of security services. In a recent ECAR research bulletin, Emory University’s Academic and Administrative Information Technology Security Lead Jay Flanagan (2006) outlined some of the many security services provided by Emory’s central IT unit, including

- e-mail virus scanning at the gateway,
- border firewall and secure network segments,
- an intrusion prevention system (IPS),

- self-service and Web application vulnerability scanning, and
- spam filtering.

Emory College has benefited—and continues to greatly benefit—from all of the services noted above. When combined with central IT’s offerings, the college’s security efforts reduce its potential exposure to attack and compromise. Indeed, the college subscribes to the observation of Notre Dame University’s Gordon Wishon that decentralized units often are very appreciative of the central IT efforts because “they are often left with the responsibility and the tasks of cleaning up from incidents, virus attacks, or worms” (Pirani, 2004, p. 7).

Chapman stated, “I appreciate the fact that the university has secured the border network over the past several years. We absorb the indirect benefits of the border firewall, IPS, and other central security services.”

Emory’s Goizueta Business School, on the other hand, has implemented its own firewall and e-mail antivirus scanning tool. Business School CIO Barbara Maaskant noted, “They [central IT] are the front line, and we don’t expect them to deal with internal risks for us. Our own services are enhanced by their offerings.”

Emory’s Rollins School of Public Health has its own firewall in order to remain in compliance with HIPAA regulations. However, central IT manages the firewall and the school itself determines firewall policies.

The choice of when and how to leverage existing central IT security services is a function of the needs of the school, as well as the existing security service offerings. Some unit-level offerings might be necessary to augment or enhance existing services. This decision will rely heavily on defining the scope of the strategy and on knowing the environment that is being secured.

The Challenge of Research Computing

Research computing presents the most unique challenge to higher education IT security. Researchers might, out of necessity, create their own small-scale IT infrastructure to support their research endeavors. When implementing a proprietary computing infrastructure, security is rarely top of mind for a principal investigator (PI). In many cases, there may be research equipment that is outdated and cannot be secured. It is not uncommon to find that research computers are still running operating systems that are more than 10 years old. These machines are necessary for operating the equipment that is attached to them and moving forward with research. If research computing falls under the scope of the security strategy, it will be important for the school to provide guidance to PIs on securing their equipment. Research data are invaluable, and their integrity and safety are of the utmost importance. Georgalis reflected that acceptance of security measures among faculty “involves grassroots buy-in.”

Buy-in from the research faculty may be slow in coming at first; however, the benefits of a secure research environment are plentiful, and that security allows PIs to focus on what is really important to them—the pursuit of the research process itself.

Dedicate Resources and Time

The security landscape is ever-evolving, and emerging threats and technologies combined with the needs of the university and users will always drive new security needs. Security strategy development is an ongoing process that must adapt to the changing IT world. For this reason, local support providers at each school must dedicate time and resources to security. It might be necessary to designate one or two personnel as security leads who are responsible for security planning, implementation, and incident response. Interestingly, Pirani (2004) found that decentralized security personnel account for a large majority of the total security personnel within institutions of higher education.

Ince noted that “It’s more difficult to approach security without someone in a lead security role.” While Emory’s business school doesn’t have a dedicated security lead, it does build security into its support routines. The school’s strategy is guided by employing best practices, staying up-to-date with current information, and being proactive.

Security is not an independent IT process; rather, it is a piece of the greater whole that should be addressed at every level of IT infrastructure. Emory College has found that almost every IT activity in some way relates to security and that security has become the driving force for infrastructural change. As Overcash observed, “Security is pervasive and omnipresent.”

Any school that develops a security strategy must determine the resources and time it wants to devote to best support the task of maintaining a secure environment.

Define the Implementation

After all of the planning stages have been completed, the technical implementation of the security strategy can begin. Available resources, existing services that can be leveraged, the institutional environment, and different computing needs and platforms will all play a major role in the ultimate technical outcome of a security strategy.

Any security strategy worth its merits doesn’t stop with the technical implementation. Relying solely on technology to solve security problems could result in less than spectacular results. The value of grass roots buy-in and the relationship with faculty and staff cannot be overestimated. This relationship can act as a springboard for greater security awareness and acceptance among users.

What It Means to Higher Education

The implications of a secure academic environment reach far beyond typical IT goals. A more secure computing environment within Emory College has helped strengthen the comfort level faculty have with technology and has allowed faculty to expand their use of technology for both research and instruction. This, in turn, has inspired Emory College to move toward a more proactive, less reactive support model. IT can now add real value to the college and provide a greater focus toward helping faculty members use

technology in a way that further promotes the goals of the college and university at large. Without security, the computing resources and investments of the institution are at high risk. One of the stated goals in the strategic plan for Emory College (2005) is to:

Invest in infrastructure that supports the teaching and research mission of the College, including technological resources that will allow faculty, students, and staff to research, teach, and communicate in innovating and effective ways. (p. 6)

The strategic plan for Emory University (2005) states that:

We must also invest in infrastructure, in our library and computing systems, to meet the growing demands of a College community that thrives on knowledge and connection. (p. 20)

...provide state-of-the-art computational and information technology resources supporting campus-wide research and learning environments. (p. 51)

Develop and maintain a state-of-the-art information technology infrastructure that is fully staffed by highly skilled professionals. (p. 54)

A secure environment also means that individual local support providers can do more with less. Taking care of basic security issues such as virus scanning, patch management, remote access, and standard secure machine configurations frees desktop support staff to pay greater attention to individual faculty and staff needs. This has been especially important to Emory College, where our computer to IT support personnel ratio is nearly 207:1.

Key Questions to Ask

- What are we trying to secure at the local level?
- What threats do we need to protect against?
- What parts of the IT infrastructure are local IT units responsible for securing? What parts of the IT infrastructure is central IT responsible for securing?
- Who are our customers, and what are their needs?
- How can we leverage existing central IT resources and services in support of local IT units?
- How can central IT and local IT collaborate on matters of security and strategy?
- In what ways does our IT security strategy serve the strategic goals of the department, college/school, and institution?

Where to Learn More

- Kvakik, R. B., & Voloudakis, J. (with Caruso, J. B., Katz, R. N., King, P., & Pirani, J. A.). (2003). *Information technology security: Governance, strategy, and practices in higher education*. (Research Study, Vol. 3). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>
- Luker, M., & Petersen, R. (Eds.). (2003). *Computer and network security in higher education*. San Francisco: Jossey-Bass, Inc.

Acknowledgments

The author wishes to thank the following five individuals from Emory University for their contributions to this research bulletin: Ben Chapman, Assistant Dean for Information Technology at Emory's School of Law; Andrea Georgalis, Senior IT Project Manager for Emory's School of Medicine; Ernesto Ince, Manager of Information Technology for Emory's Woodruff School of Nursing; Barbara Maaskant, CIO of Emory's Goizueta Business School; and Marc Overcash, CIO for Emory's Rollins School of Public Health.

References

- Boes, R., Cramer, T., Dean, V., Hanson, R., & McKenna, N. (2006, August 15). *Campus IT security: Governance, strategy, policy, and enforcement*. (Research Bulletin, Issue 17). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>
- Emory College. (2005). Traditions and transformations: A plan to guide the future of Emory College. Retrieved September 5, 2006, from http://www.college.emory.edu/about/planning/strategicplan_overview.pdf
- Emory University. (2005). Where courageous inquiry leads... Strategic Plan: 2005–2010. Retrieved September 5, 2006, from https://admin.emory.edu/StrategicPlan/reports/StrategicPlan4.11.06/EU_Plan_03.28.06.doc
- Flanagan, J. (2006, March 28). *Surveying the steps to a secure Emory University*. (Research Bulletin, Issue 7). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>
- Kvakik, R. B. (with Voloudakis, J.). (2006). *Safeguarding the tower: IT security in higher education 2006*. (Research Study, Vol. 6). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>
- Pirani, J. (2004, March 16). *High stakes: Strategies for optimal IT security staffing*. (Research Bulletin, Issue 6). Boulder, CO: EDUCAUSE Center for Applied Research. Available from <http://www.educause.edu/ecar/>

About the Author

Derek Spransy (derek.spransy@emory.edu) is the IT Security Lead for Emory College, Faculty of Arts and Sciences, at Emory University.

Copyright 2006 EDUCAUSE and Derek Spransy. All rights reserved. This ECAR research bulletin is proprietary and intended for use only by subscribers. Reproduction, or distribution of ECAR research bulletins to those not formally affiliated with the subscribing organization, is strictly prohibited unless prior permission is granted by EDUCAUSE and the author.