OKLAHOMA STATE UNIVERSITY™

Information Technology Division

The Office of IT Systems Security

Staffing Assessment

July 2003

Table of Contents

List of Figures

List of Tables

Executive Overview

Universities are not immune to the very real and often critically damaging threats to IT security. Rather, they are among the systems most frequently targeted by hackers. This is because university IT systems and networks are traditionally very open and accessible to allow students and faculty maximum access to cutting edge technology resources. Also, in many cases, universities have been slow to realize the potential for attack inherent in higher education IT systems and to make IT security a main priority.

With advancements in computerized data collection and analysis in all fields of research comes an increasing need to ensure the protection of this valuable and often sensitive data. Likewise, online course management and other administrative systems must be secure. Disabling access due to an attack interferes with critical administrative activities and impedes students' academic work. Further, demand for administrative systems uptime has increased, and there is a growing expectation that services and systems be constantly accessible (McRobbie, IT Security in Higher Education).

The Office of IT Systems Security provides varying levels of IT security support to the OSU/A&M system ranging from communicating vulnerabilities and intrusions to conducting full computer forensics investigations. However, the demand for IT systems security services continues to escalate based on legal requirements and the number of threats introduced into the environment as well as the ever-increasing quality of available hacking tools and programs. Implementation of security standards and best practices are required to mitigate risk to the university. The ability to meet the growing demand for service is based on available resources. Security tools have been acquired but require manpower to configure, monitor, and maintain, and testing of new tools is limited.

In order to protect OSU and the system from IT security incidents it is necessary to allocate more manpower to provide adequate service. The current staff is composed of two full time employees who are dedicated to security management. One additional full time telecommunications employee allocates a portion of his time to security. It is recommended that additional resources be allocated to focus on IT security.

This report outlines the need for additional staffing that would enable OSU IT Division to become a national leader in the area of IT Systems Security. The current national leader for higher education IT Systems Security is Indiana University. Indiana University currently has a staff of 21 security professionals. We recognize that in such a tight budget year it will be impossible to advance quickly to national leadership status, however, we still recommend that an additional two full time personnel be added to the staff. We recommend that where possible, reallocation of existing staff be the solution. However, existing staff may not have the qualifications necessary to provide the service required.

Introduction

Historically, the culture of higher education IT has been to provide academic freedom by allowing full access to all non-administrative computing resources. This has begun to shift to a less open environment in order to provide the institution protection from hackers, to eliminate theft of intellectual properties, and to provide a high security solution for research requirements. Higher education networks are viewed as a prime target for hackers because of the power and wide open nature of university computing resources.

The need for information technology security has steadily increased over the past six months. The number of vulnerabilities and attack attempts continues to escalate. The Office of IT Systems Security is striving to reach the necessary level of protection by acquiring sophisticated security tools to detect, prevent, and monitor malicious network activity.

Information to develop this report was gathered by polling other universities, researching best business policies, and analyzing current status versus desired state for OSU security. The result of the research was the discovery that all organizations are struggling to meet the growing demand for IT security given the current economic situation. Addition of staff is difficult, and most institutions are reallocating staff to meet the need.

Current Status

The Oklahoma State University IT Systems Security Office in collaboration with the Telecommunications Department has made great efforts to secure the OSU network and computing infrastructure; however, much more progress is needed. Major investments and improvements have been made by implementing intrusion detection systems, firewalls, incident response, and antivirus infrastructure. These tools have increased the level of protection but have not been fully exercised. With the addition of tools comes the need for personnel to maintain, monitor, and tweak the systems in order to mitigate risk. OSU has not added additional personnel to focus on security related issues since 2001. The IT Systems Security Office operates in reactive mode and is struggling to provide service to the institution. The OSU system is in dire need of additional security focused personnel. Security services cannot be increased without additional manpower.

The Office of Information Technology Systems Security was created in March 2001 with the addition of a Systems Security Officer (SSO). This was created as an administrative position with emphasis on security policies. Concurrently with the SSO, a position was created within Network Operations to fulfill the technical needs of the security office. The creation of these two positions meant that two full-time equivalent (FTE) were responsible for managing and conducting all computer and network security related functions. Two FTE did not meet the necessary manpower levels to effectively carry out all security functions. Their major areas of responsibility included,

- Drafting security policies
- Implementing an intrusion detection system
- Conducting rudimentary incident response
- Providing security procedure advice
- Tracking exception information access

- Tracking and managing security incidents

In December of 2001 an additional person was added to conduct an increased level of incident response, computer forensics, and security awareness training. Many security services requiring two to three FTE are currently carried out by a single individual who has multiple job functions. Security personnel can barely scratch the surface of what is needed to conduct an in-depth task (Figure 1).

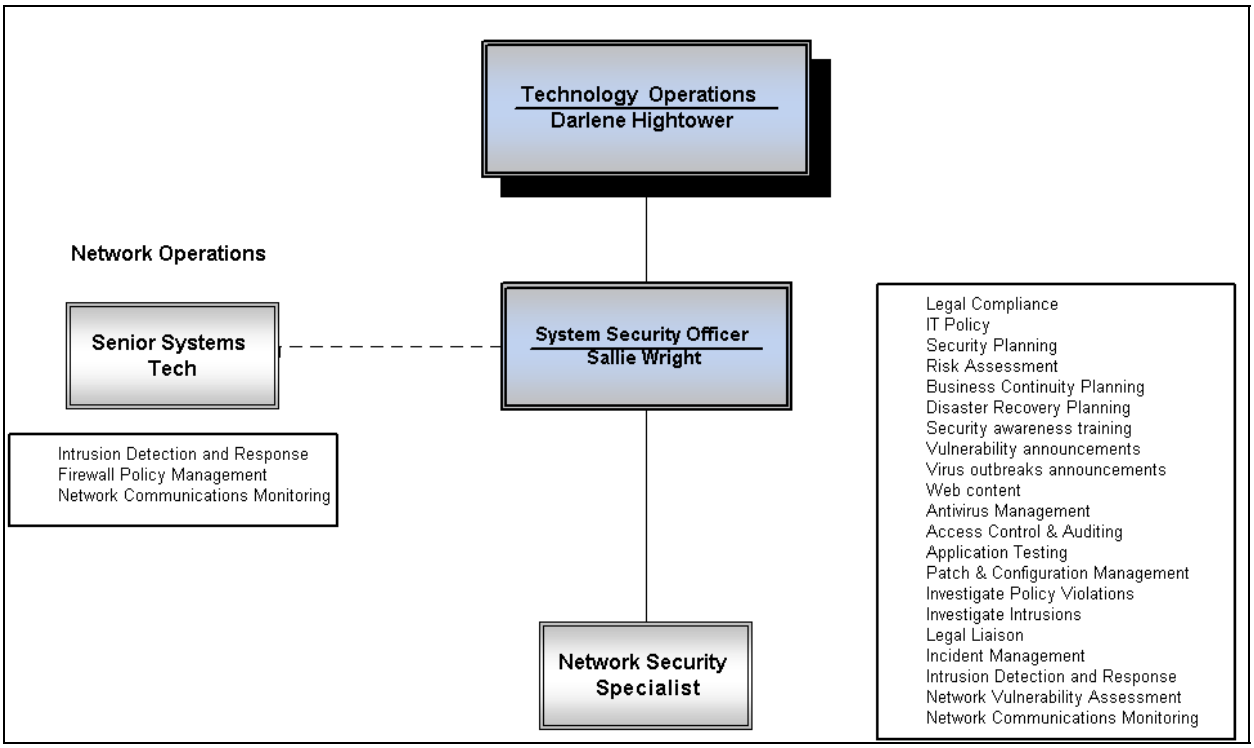

Figure 1 – Current Operations

Many security functions are performed by various organizations across the system. This decentralization results in a lack of global access control. There is no one point of contact where access can be added, changed, or deleted as needed. Users are forced to gain access to systems by contacting multiple system administrators, and managers are unable to quickly eliminate access when terminations occur. Access to the network is controlled by IT LAN Systems and the HelpDesk. Human Resource Systems (HRS), Financial Resource Systems (FRS), and Student Information Systems (SIS) all have respective access control personnel and are not centrally managed. Servers are not currently registered and departmental applications are controlled by departmental system administrators. Centralization of security functions would enable standardization of server and workstation security as well as a single point of contact for global access control.

Since the end of 2001 the need for more security services has risen with the increase in hacker activity and statutory requirements such as HIPAA and GLBA (Figure 2). The IT Systems Security Office has tried to meet the demands of the campus by continuing to add services, but additions have come at the expense of existing duties.

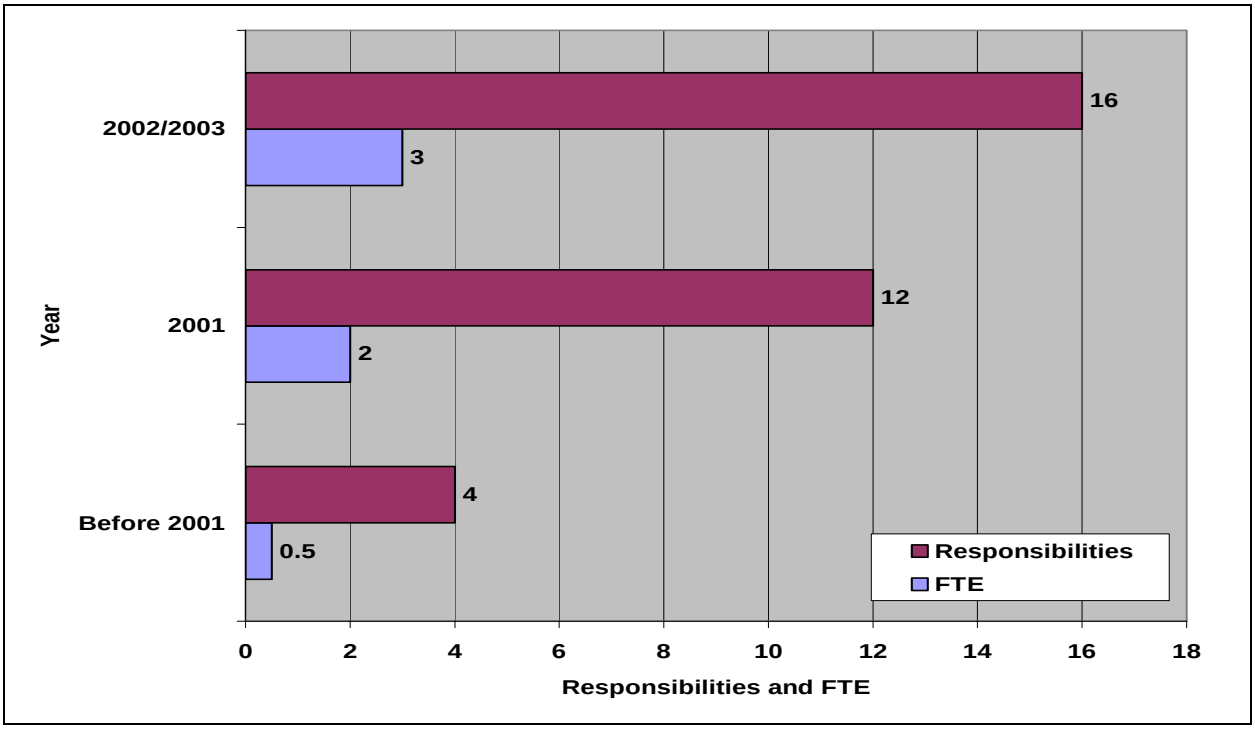

Figure 2 – Number of Responsibilities versus Number of FTE

The number and sophistication of attacks have increased as the knowledge needed to carry out the attacks has decreased (Figure 3). The number of vulnerabilities of operating systems and applications has also increased.

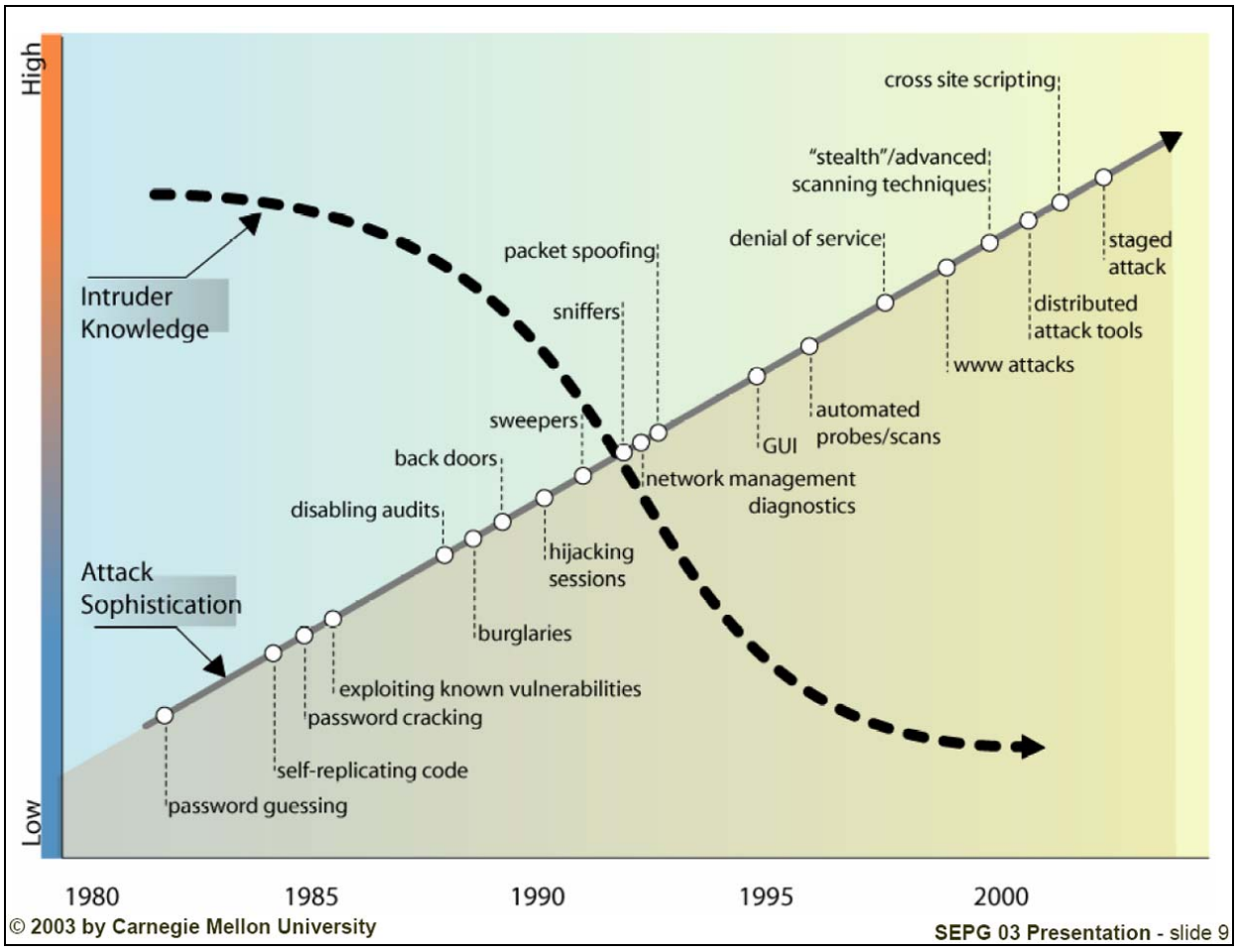

Figure 3 – Intruder Knowledge versus Attack Sophistication

Because of these global trends, the OSU network has seen an increase in network intrusions — including compromised hosts, viruses and worms, and network probes — from 30 in August of 2002, to 340 in March of 2003 (Figure 4). During the month of June 2003 the network saw an average of 1.3 million network probes per week.[1] All of these threats could be minimized if the IT Systems Security Office had the personnel to use existing technology to its fullest extent.

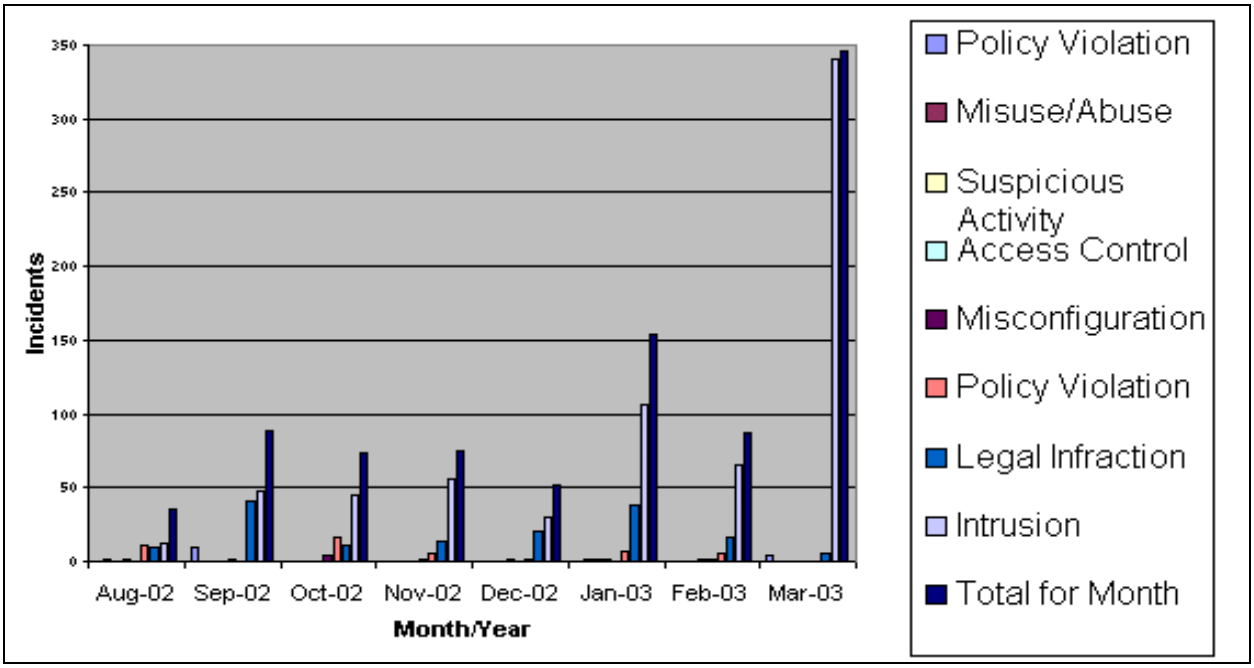

Figure 4 – Incidents August '02 – March '03

The IT Division has invested financially in several systems to enhance security and incident response. The IT Division and campus networks would be more secure if these products were used to their full potential. These systems are complex and need to be constantly monitored and re-configured to mitigate evolving threats. The systems include,

- EnCase's Computer forensic software
- Internet Security Systems' enterprise class intrusion detection system
- NetIQ's Active Directory Administrative Suite
- Microsoft's Software Update Service
- Netscreen's 5200 series firewall

[1] Snort portscan statistics from 05-29-2003 to 07-03-2003 averaging top ten scanned ports.

In addition to managing security technologies, the IT Systems Security Office has taken on the following security management responsibilities.

- Security awareness training
- Security website communications
- HIPAA security plan
- Business continuity planning
- Disaster recovery planning

The IT Systems Security Office has provided computer forensics across the A&M system. Each case requires significant time and analysis. With recent strategic changes in IT, new responsibilities will be added to include the other campuses within the OSU system with great emphasis on the medical facilities and bio-terrorism research. The IT Division security personnel currently have difficulty meeting the expectations of the OSU-Stillwater users and will experience acute shortages when security services are provided to other campuses. The IT Systems Security Office will be involved heavily in business continuity planning in the near future to meet compliance requirements for HIPAA, GLBA, and bio-terrorism research.

Recommendations

The Office of IT Systems Security recommends using a phased approach to increase security staff.

Phase One

To meet the immediate needs of the Stillwater campus five additional professionals are required. Reallocation of resources in combination with external hires is the preferred method to increase resources. These resources would meet critical needs in the following areas: business continuity, network security (firewalls and intrusion detection/prevention), incident handling, access control, identity management, and faculty research system security requirements. Table 1 and Appendix A detail a complete list of responsibilities.

Security Domain	Current FTE	Phase One		Phase Two		Benefits
		Add	*Total*	*Add*	*Total*	
Access Control Systems and Methodology	0.10	0.50	0.60	1.00	1.60	Global Access is required for HIPAA, Server Registration
Applications and Systems Development Security	0.25	0.50	0.75	1.00	1.75	Antivirus, Patch Management, Penetration Testing, Application Development Testing
Business Continuity and Disaster Recovery Planning	0.10	1.00	1.10	0.50	1.60	HIPAA, Bioterrorism, Campus
Cryptography	0.00	0.25	0.25	0.75	1.00	Identity Management and VPN
Law, Investigation, and Ethics	0.50	1.00	1.50	0.75	2.25	Forensics, Incident Management
Operations Security	0.00	0.25	0.25	0.50	0.75	Standards, Threat Analysis, Records
Physical Security	0.00	0.00	0.00	1.00	1.00	Network Devices, Critical Servers
Security Architecture and Models	0.00	0.25	0.25	0.50	0.75	Consistent Standards
Security Management Practices	0.75	0.50	1.25	1.50	3.00	Policies, Communications, Training
Telecommunications and Network Security	1.30	0.75	2.05	1.50	3.55	Firewall, IDS, IPS
Totals	**3.00**	**5.00**	**8.00**	**9.00**	**17.00**	
Current = 3 FTE, (Includes 1 Telecommunications person)						

Table 1 – Recommended Personnel Additions by Domain

The IT Systems Security Department should be organized into two distinct areas of responsibility, Operational / Technical Security and Security Management, in order to maintain proper separation of duty (Figure 5).

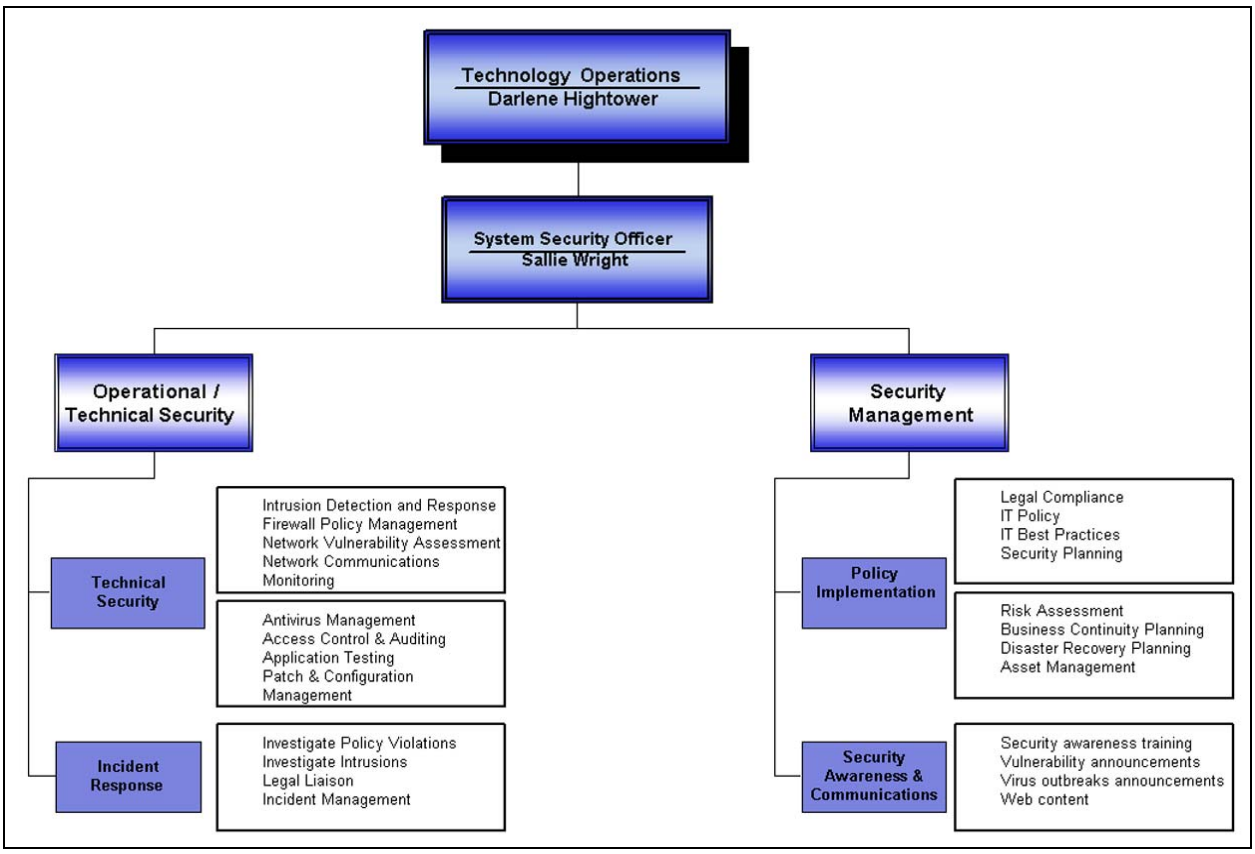

Figure 5 – Department Organization by Responsibility

Phase Two

To address the security needs of the A&M system, an additional nine FTE will be needed. Once again, reallocation and new hires is the recommended method to meet this resource need. The second phase of staffing should occur over the course of several months. The areas of responsibility not addressed in the first phase would be host security, application security, and physical security. It is also recommended that additional personnel be assigned to network security, incident response, and security management. Organizationally, the department will be composed of three distinct areas: technical security, operational security, and security management (Figure 6).

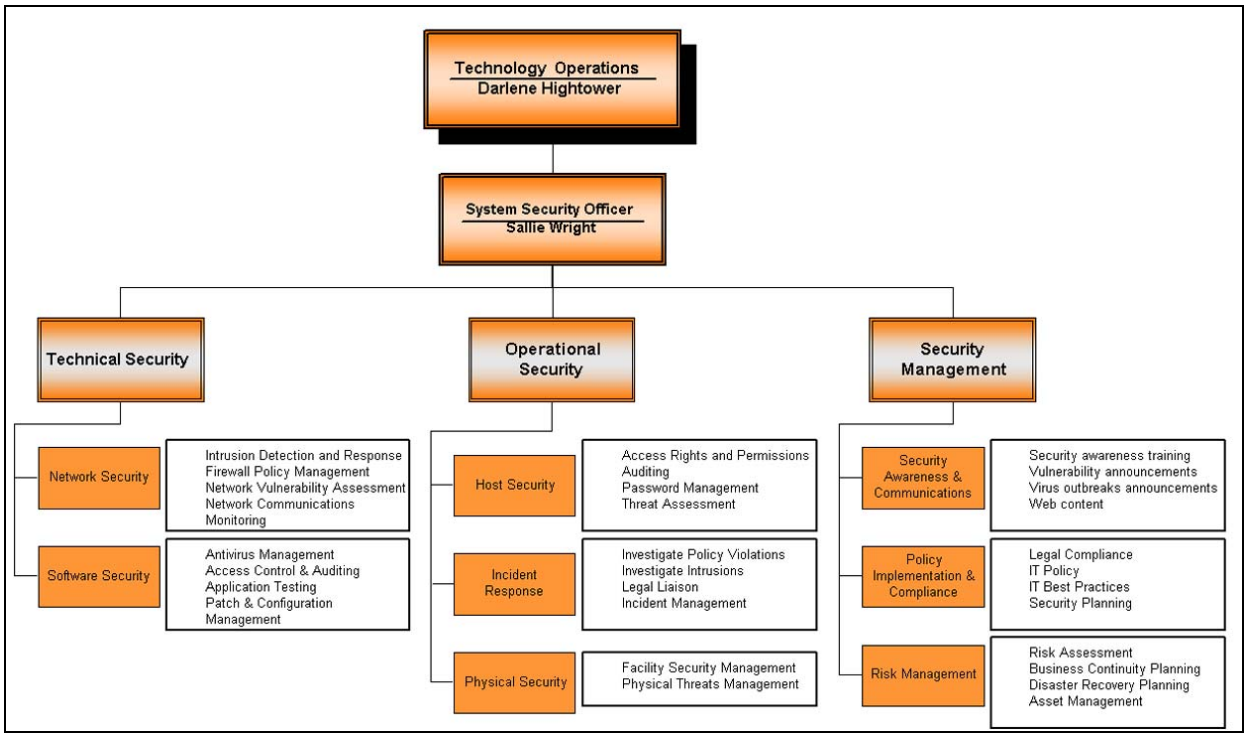

Figure 6 – Department Organization by Area

Conclusion

Failure to increase staffing poses significant risk to the university and the system. Computer crime continues to grow as do the legal compliance requirements. Staffing costs are insignificant compared to the costs of a law suit or a criminal or civil suit from an HIPAA violation. OSU leadership must recognize that information technology is ingrained in all academic and administrative activities and that poor system, network, and data security will have a direct and costly impact on OSU's mission (McRobbie).

Appendix A – Roles of Security Personnel

Domain / Responsibility	Category	Role
Security Management Practices		
Implement policies and procedures	Management	Security Management Manager
Risk management	Management	Security Management Analyst
Asset management	Management	Security Management Analyst
Security awareness and communications	Management	Training and Communications Specialist
Security management planning	Management	Security Management Manager
Access Control		
Access rights and permissions auditing	Operational	Host Security Analyst
Access control policies / procedures / standards	Management	Security Policy Specialist
Authentication and password management	Operational	Host Security Analyst
Manual and automated removal processes	Management	Security Policy Specialist
Telecommunications and Network Security		
Firewall policy management and auditing	Technical	Network Security Analyst
Intrusion detection policy management and auditing	Technical	Network Security Analyst
Network communications security management	Technical	Network Security Analyst
Intrusion response and investigations	Operational	Network Security Analyst / Incident Handler
Network vulnerability assessment	Technical	Network Security Analyst
Cryptography		
Application cryptographic functions	Technical	Software Security Analyst
Network-based cryptographic functions	Technical	Network Security Analyst
Storage cryptographic functions	Technical	Software Security Analyst
Hardware cryptographic functions	Operational	Host Security Analyst
Security Architecture and Models		
Security systems design and planning	Management	Security Management Manager / Security Analysts
Certification and accreditation	Management	Security Management Manager / Security Analysts
Operations Security		
Administration management	Operational	Operational Security Manager
Resource protection	Operational	Technical / Operational Security Managers
Security controls management	Operational	Operational Security Manager
Threat and vulnerability analysis	Operational	Technical / Operational Security Managers
Countermeasure management	Operational	Technical / Operational Security Managers
Records management	Operational	Security Documentation Specialist

Domain / Responsibility	Category	Role
Applications and Systems Development		
Antivirus management	Technical	Software Security Analyst
Applications vulnerability assessment	Technical	Software Security Analyst
Applications development testing	Technical	Software Security Analyst
Database security assessment	Operational	Host Security Analyst
Patch and configuration management	Operational	Software Security Analyst
Business Continuity Planning		
Planning, preparation, testing, and BCP and DRP	Management	Security Management Analyst
Law, Investigation and Ethics		
Law enforcement and legal liaison	Operational	Operational Security Manager
General investigation	Operational	Incident Handler
Incident handling	Operational	Incident Handler / Security Analyst
Forensic investigation	Operational	Incident Handler
Evidence handling	Operational	Incident Handler
Physical Security		
Facility security management	Operational	Physical Security Specialist
Physical threats management	Operational	Physical Security Specialist

References

Allen, Julia H. *What is My Role in Information Survivability? Why Should I Care*? 2 April 2003. Carnegie Mellon University. 15 July 2003. <http://www.cert.org/archive/pdf/info_surv_pres040203.pdf>.

Information Technology Security Office: About the ITSO. 2003. Indiana University. 16 July 2003. <http://www.itso.iu.edu/about>.

Information Technology. 2003. Indiana University. 16 July 2003. <http://www.indiana.edu/%7Eovpit/ovpit.html>.

IT Policy Office. 11 July 2002. Indiana University. 16 July 2003. <http://www.itpo.iu.edu/staff.html>.

Krutz, Ronald L., and Russell Dean Vines. The CISSP Prep Guide: Gold Edition. Indiana: Wiley, 2003.

McRobbins, Michael A. "IT Security in Higher Education." Lecture at 2003 Secure-IT Conference Temecula, California.

Tipton, Harold F., and Micki Krause, eds. Information Security Management. Vol. 4. 4th ed. Boca Raton: CRC, 2003.