INFORMATION TECHNOLOGY SERVICES

INFORMATION RISK MANAGEMENT PROGRAM

The Need for a Risk Management Program

Information Security & Privacy Office

June 8, 2017

Why Unit Risk Management Programs Are Important

For the most part FSU has enjoyed wide academic freedom with respect to how we processed, stored, transferred, and protected information received from government and private entities; however, laws and contractual requirements are increasingly specifying the implementation of auditable security and privacy controls prior to the receipt of information. A key component in this shift mandates a risk management program as a methodology to preserve the confidentiality, integrity, and availability of information. In addition, ***a functional risk management program supports efforts to uphold the trust and confidence in your unit and the university by***:

✓ **Protecting Research Funding**

✓ **Protecting Research Information**

✓ **Protecting Connected Research Equipment**

✓ **Protecting Intellectual Property**

✓ **Protecting Patient Information**

✓ **Protecting Student Information**

✓ **Protecting Alumni Information**

✓ **Protecting Donor Information**

✓ **Protecting Vendor Information**

✓ **Protecting Customer Information**

✓ **Protecting Financial Information**

✓ **Protecting Information Processing Assets**

✓ **Meeting Contractual Obligations**

✓ **Meeting Legal Obligations**

Examples of University IT Control Failures

Universities are targeted by cyberattacks every day. The following pages document real-life examples of successful security and privacy breaches at national universities, each resulting in considerable monetary loss or service disruption. The various case studies emphasize the importance of adopting a robust risk management program, and the imminent threats if insufficient safeguards are in place.

Research Breach

University of North Carolina (UNC)

Event | UNC discovered that servers used for a mammography research program had been compromised. This placed the medical research data, including Social Security numbers, of more than 180,000 women at risk. (2010)

Background | The compromised servers were supporting a cancer research project headed by Dr. Yankaskas, a professor in the Department of Radiology and principal investigator of the project. She was cited for hiring an underqualified systems administrator and failing to provide the administrator with training to properly deploy security and privacy controls to protect research information in the study. In addition, it was noted Yankaskas obtained sensitive HIPPA-protected patient data from UNC Hospitals without proper authority. Ultimately, the university ruled that the principal investigator is responsible for the security of project information with which they are entrusted.

Consequences | Originally, Dr. Yankaskas was dismissed from the university; however, after appealing her dismissal, Yankaskas was demoted from full professor to associate professor with tenure. In addition, the university reduced Yankaskas' salary from $178,000 to $93,000. UNC notified 180,000 individuals involved in the breach, costing the university $250,000.

Failure to Properly Categorize and Protect Unit Data

University of Massachusetts at Amherst (UMass)

Event | UMass failed to properly identify all of its component organizations that handled electronic protected health information (ePHI) subject to federal HIPAA rules. One of the misidentified groups, the Center for Language, Speech and Hearing, was later hacked, compromising the records of 1,670 people. (2016)

Background | Per the Office for Civil Rights (OCR), UMass failed to designate the Center for Language, Speech and Hearing as a HIPAA-covered health care component. Therefore, it had not implemented policies and procedures at the Center to ensure compliance with HIPAA Privacy and Security Rules. OCR investigators also noted UMass failed to implement technical security measures (firewalls) to guard against unauthorized access to ePHI transmitted over an electronic communications network. In addition, UMass was cited for not previously conducting an accurate and thorough risk analysis.

Consequences | UMass agreed to pay a $650,000 fine to settle the case alleging it failed to properly identify all of its component organizations that would handle electronic protected health information (ePHI). In addition, UMass agreed to:

- Conduct an enterprise-wide risk analysis
- Develop and implement a risk management plan
- Revise its policies and procedures and retrain its staff

Unit Server Breach

University of Wisconsin-Madison (UW)

Event | A database in the UW Law School was the target of computer hacking and leaked students' personal information. (2016)

Background | The compromise targeted a database that contained names and Social Security numbers of UW Law School applicants from 2005-2006. Security measures have been increased, including implementing additional vulnerability identification programs, evaluating current computer applications and decommissioning those no longer needed, tightening credentials for access to databases and deploying additional network intrusion detection.

Consequences | Notices were forwarded to 1,213 people affected by the hack who received free credit monitoring for one year to help protect them against identity theft. The total cost of the breach response actions was not released by the university; however, the average contracted price for credit monitoring is $25 per person, equaling $30,325 for this event, plus the cost of staff response time.

Michigan State University (MSU)

Event | Hackers gained unauthorized access into an MSU database containing names, Social Security numbers and other identifying information. An email from the alleged hacker seeking money to not reveal the information arrived on Nov. 13, 2016, alerting the university to the data breach. (2016)

Background | Names and MSU identification numbers of 400,000 users were exposed along with Social Security numbers. An internal investigation identified 449 users whose information was viewed by the unauthorized individual(s). The affected individuals included faculty, students and staff employed by MSU between 1970 and 2016, and others who were students between 1991 and 2016.

Consequences | Between providing identity protection and enhancing its security systems, MSU estimates it will spend $3 million in response to the attack.

Unit Network Disruption

Massachusetts Institute of Technology (MIT)

Event | Since the beginning of 2016, the (MIT) network has been assaulted at least 35 times by distributed denial of service (DDoS) attacks. DDoS is a cyberattack where the perpetrator attempts to make an online service unavailable by flooding it with superfluous requests and overloading the system with traffic. (2016)

Background | The DDoS campaigns have been aimed at different targets within MIT, and roughly 43% of the attacks leveraged DDoS reflection and amplification methods (using worldwide compromised IT resources to power the attack). Attackers targeted multiple destination IPs within the MIT network during these incidents and used a combination of devices to launch the attacks.

Consequences | Each attack caused the affected IP(s) in the MIT network to lose Internet access or have markedly slow Internet response times. Lack of Internet access disrupted administrative, research and classroom activities.

Pennsylvania State University

Event | The Federal Bureau of Investigation (FBI) informed Penn State that the College of Engineering’s network had been breached by two cyberattacks. Attackers had placed malware on machines and gained unauthorized access to the college’s network and computing devices. (2015)

Background | The university responded to the attack by blocking Internet access to the engineering network for three days as it worked with the IT security firm FireEye to set up “robust scanning and computer security protocols” to “take a proactive and aggressive stance against future attempted intrusions.” Further investigations revealed two more attacks against the College of Liberal Arts. As opposed to the engineering school attacks, where hackers used malware to gain access to the network, the College of Liberal Arts network was breached by exploiting a vulnerability.

Consequences | The College of Engineering was cut off from Internet access for a three-day period disrupting college, research and student communications.

Bank Account Redirect

Western Michigan University (WMU)

Event | Ray Cool, an assistant professor for WMU in the College of Education, had his *GO WMU* portal account hacked. The hackers signed in to his university account and reset his direct payroll account information to an account they controlled in a Utah-based bank. (2014)

Background | It appears the professor fell for a phishing email and provided his *GO WMU* sign in credentials to the unauthorized individuals by clicking a link to a fake WMU website. The unauthorized individuals then signed in to his account and changed Cool's bank routing information in the online portal. The automatic payroll process used the altered routing information and his $1,581 direct deposit paycheck was forwarded to the bank in Utah.

Consequences | The crime was traced to a computer in New Mexico, but WMU authorities were only able to recover $11.08 of Cool's paycheck. The professor was told WMU would not reimburse him for the amount that was stolen. WMU contended a confirmation notice of the change was sent to his email, and. Cool's lack of a response to that email left him liable for the breach of his account.

Data Manipulation: An Imminent Threat

It is important to understand the risks data manipulation presents to FSU.

Beyond the traditional breaches highlighted above, experts warn that attackers are poised to launch sophisticated campaigns designed to manipulate financial, healthcare, research and government data to covertly disrupt the US information infrastructure.

The following represents a simplified example a university data manipulation attack that would affect the reputation of the faculty, staff and university.

> *Through the deployment of a stolen user password, an adversary is able to penetrate the network perimeter of a unit. Due to lack of proper network segmentation, the hacker immediately proceeds to the unit's digital treasure chest: research databases. Soon thereafter, the undetected visitor gains access to a database that houses data for a federally-sponsored weather research project. Once inside the database, the hacker begins to systematically alter the repository's tables. The manipulation is performed over a multiple-month period to skew weather forecasting data used to predict US corn production. Since the data used for the research is considered public data, the researchers have not identified the databases as high risk nor instituted a higher level of control to protect data integrity. Knowing the data will skew the university report in their favor, the hacker makes corn financial futures market bets that pay off when the flawed university research is published. When the manipulated research information is discovered, the university and research team experience reputational damage for not properly safeguarding the data.*

About the Information Security & Privacy Office

Florida State University takes seriously its obligation to respect and protect the privacy of the campus community and to safeguard the confidentiality of information important to the university's academic and research missions. The Information Security and Privacy Office is responsible for preserving and enhancing privacy protections for all students, faculty, staff and alumni.

Contact Us

Information Security and Privacy Office
Information Technology Services
security.fsu.edu

Brian Rue, Associate Director
850-645-8056
brue@fsu.edu