Anish Nag

Jeff Franklin

CybE 234

02 May 2024

CISO Risk Assessment Breakdown

Being the Chief Information Security Officer for Iowa State means I have been assigned the responsibility of ensuring the security of this institution's most critical information and IT assets. To accurately assess Iowa State's current security posture, it is crucial for the university to conduct thorough testing of its network, assets, and infrastructure, also known as a risk assessment. This evaluation will provide a clear overview of our security capabilities and resilience against cyber attacks. My approach to creating a robust risk assessment for Iowa State entails a systematic and comprehensive approach where I need to identify, prioritize, and manage risks based on their potential impact on the university's assets, operations, and reputation. More specifically, the IT assets I want to protect heavily include student data, research data, and the university's network infrastructure. A strong method of approach is required to assess the possibilities of risk, therefore I will utilize the STRIDE methodology to assess possible threats, identify potential threat actors, and deliberate the level of impact of these threats if realized.

At first thought, my primary concern was the protection of student data. At Iowa State University, students expect their personally identifiable information (PII), financial details, and academic and health records to be confidential. Using the STRIDE framework learned in lecture from the Threat Modeling PowerPoint, which includes Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege, it becomes clear that

Information Disclosure, Tampering, and Denial of Service are especially crucial to address. Information Disclosure is critical because it breaches confidentiality when sensitive data is accessed without authorization. This can lead to targeted attacks and potential identity theft. Tampering threatens data integrity, making records like academic achievements inaccurate and unfair. Lastly, Denial of strategies blocks access to critical student systems, making it difficult for students to retrieve essential information like transcripts. In week 10 lectures, we learned about various types of threat actors. Disgruntled students and cybercriminals who yearn for financial gain are two types of bad actors who would strive to access this data. Students who aren't happy with the university could seek revenge for whatever has been done to them. Cybercriminals can profit from either using financial PII or selling it. These security issues could severely damage Iowa State University's reputation, potentially causing a decrease in enrollments and prompting current students to leave. Therefore, protecting against these threats is vital for maintaining trust and ensuring the university remains a secure place to study.

Ultimately, most campus operations would halt if the Iowa State network went down. The network infrastructure of Iowa State is the core IT infrastructure that supports network connectivity, internet access, administrative operations, and security systems across campus. Out of the STRIDE methodology, we would focus most on Spoofing, Repudiation, Denial of Service, and Elevation of Privilege. Hackers can spoof by impersonating network components to reroute or intercept traffic. They can intercept sensitive communications that could have important data in them. Looking for poor log management for repudiation is essential because logs provide proof of any incidents. Hypothetically, if an attacker got in, having organized logs would show how they got in, which could be used for future mitigation strategies. Regarding a DoS attack on

the Iowa State network, crucial systems function and communication would be affected, stopping to prevent other smaller operations from happening. Preventing areas of privilege escalation will prevent hackers from reaching a privilege where they can control network resources. Once an actor has reached administrator privileges of a network, they could do permanent damage at the worst and keep the network down for as long as they wanted. On top of that, they would access any information on that network. The primary actors I see conducting a network attack are hacktivists and malicious/disgruntled students and employees. If Iowa State were involved in some business that a hacktivist did not approve of, they would do what it takes to prevent it from happening or send a warning. For a student if something occurred during a student's time at the college that set them off, they could engage in an act of revenge. Overall, protecting the network infrastructure could arguably be the number one priority because of how crucial it is for the school to operate.

Lastly, Iowa State indulges in research as most colleges do; therefore, confidential research should be secured. To provide context, colleges research for purposes such as fostering innovation, technological advancement, providing students with a platform to create and publish, community engagement, and even collaboration with businesses and the government. This shows that university research is essential and has a purpose. Aspects of the STRIDE methodology that would be focused on are Tampering, Information Disclosure, Denial of Service, and Elevation of Privilege. Regarding tampering, it violates integrity if research data is altered due to a bad actor. Information Disclosure comes into play because if a hacker gets access to research, they can steal it and pawn it as their own. Denial of Service happens if an actor can bring a network or system down and now the students and faculty cannot access the research they are doing. This is a

complication because it halts progress and pushes back the schedule if the research is timed deliverable. Elevation of privilege happens if an actor can privilege escalate to an administrator or user with enough privilege to access a restricted area containing the research. Two types of threat actors that would launch attacks on the research would be nation-states or even competing academic institutions. Nation-states would be interested in gaining a competitive advantage in technology or military capabilities. Competing academic institutions would want an edge on the research to get the credit for completing it faster. The overall impact is that there could be a loss of competitive advantage in research, financial losses due to the compromised integrity of research, and damage to the university's reputation and future funding.

In summary, the role of Chief Information Security Officer at Iowa State University demands a vigilant and proactive approach to safeguarding the institution's critical digital and information assets. Our comprehensive risk assessment strategy, guided by the STRIDE methodology, is essential for understanding and mitigating potential threats to student data, research integrity, and the overall network infrastructure. Protecting these assets is not merely a technical requirement but a fundamental aspect of maintaining trust within the university community, ensuring the continuity of academic and administrative operations, and upholding Iowa State's reputation as a safe and innovative educational environment. In the broader context, our efforts in cybersecurity resonate beyond the campus boundaries, influencing how future institutions will approach information security challenges. Ensuring robust protection against potential breaches and cyber attacks matters immensely, as the consequences of failing to do so could lead to a decline in student trust, compromised research, and, ultimately, a significant impact on the educational and research missions of the university. This real-world implication

underscores the importance of cybersecurity in the modern educational framework, highlighting its role in protecting and nurturing intellectual and personal growth within our university.

Works Cited

https://canvas.iastate.edu/courses/108391/pages/week-10-threat-modeling-and-risk-management?module_item_id=6171503

https://canvas.iastate.edu/courses/108391/pages/week-10-content?module_item_id=6171504