Enhancing Information Security and Privacy

Objectives

Increase funding to the Office of the Chief Information Security Officer (CISO) to help address information security and privacy risks, meet the current demands of the University, support future research, and provide consulting services to help UW colleges, school, and departments develop and enhance their information security and privacy strategy.

Strategic Context

The University's mission is dependent on dynamic technologies and an enormous volume of information for academic, research, and administrative purposes. This comes with unique security and privacy challenges, a growing threat spectrum, and compliance responsibilities. The UW Office of the CISO is building and expanding a security and privacy program that delivers trusted, reliable, and effective services for the UW community. This pragmatic risk management-based security and privacy program is key to identifying and reducing inevitable and evolving risks related to the UW.

Key Benefits

- Develop new tools and services to help identify gaps.
- Consult with UW colleges, schools, and departments regarding information security and privacy risks and potential impacts.
- Provide insight and solutions for addressing information security and privacy issues on UW's network.
- Assist units in developing strategies for managing risks.
- Support network monitoring for malicious traffic or specific information security and privacy issues.
- Develop tools that provide an understanding of risks and potential threats, and intelligence for executives and their support staff, and support for new research opportunities.

Risks

The University risks a host of potential and obvious liabilities related to information security and privacy. At the heart of the University's risk exposure is its reputation and leadership role in Higher Education and healthcare.

"Threat actors[1]" are targeting the UW in order to access cutting-edge research, intellectual property, financial information, or confidential information. The threat actors are incredibly motivated and have seemingly unlimited resources as well as sophisticated methodologies and tools.

At current funding levels, the Office of the CISO remains in a reactive and limited state of capability that only provides minimal services for the UW:

- **Gaps**: UW does not have a comprehensive and clear view of campus systems and data that cause information security and privacy pain points.
- **Incident Management**: Incidents are remediated in silos at an individual system or unit level, which makes UW susceptible to repeat incidents for identical data sources on similar or dependent systems.
- **Big Data:** Employees are combining and analyzing data sources and there is a lack of understanding about the information security and privacy implications.
- **Mobility**: Traditional control methodologies are too cumbersome for the current landscape, where technology and data that are rapidly evolving and becoming more mobile.
- **Compliance**: UW does not have a cohesive strategy for addressing 27 different laws that contain information security and privacy regulations. Federal regulators will likely increase requirements for cyber security, data protection, cloud computing, and security of research data.

With adequate funding, the Office of the CISO can develop capabilities in threat and risk awareness and predictive analytics that provides context for informed decisions about information security and privacy:

- **Intelligence:** UW and campus units are given analytics on systems and data that present information security and privacy risks. Campus units have the tools and consulting resources needed to assist them in managing risks and developing strategic plans for information security and privacy.
- **Incident Management:** Risks and incidents can be remediated at the root cause across the institution so repeat incidents are avoided.
- **Big Data:** Work with business partners and researchers to understand how they are using data, explore security implications and solutions, and support accessibility.
- **Mobility:** Develop a variety of security solutions that are flexible and can be used by campus units to meet a large variety of needs and uphold a due care position with regulators.
- **Compliance:** Prepare UW for new regulatory requirements and provide researchers with tools to evaluate, address, and properly account for security requirements in grant/contract proposals.

[1] "Threat actors" is a term of art in the security field, meant to convey the notion that responding to these threats effectively requires a good understanding of the people behind the threats, and their motivations and incentives.

Budget Request

There are two options for the IT Services Investment Board's consideration:

Option A – Fund the Office of the CISO budget to provide a comprehensive program to help address information security and privacy risks, meet the current demands of the University, support future research, and provide consulting services to help UW colleges, school, and departments either develop or enhance their information security and privacy strategy.

Description		Fiscal Year Expense
Salaries, wages, and benefits for 5 FTE	Develop new tools and services to help identify gaps; consult with UW colleges, schools, and departments on information security and privacy risks and potential impacts; provide insight and solutions for addressing information security and privacy issues on UW's network; and assist units in developing strategies for managing risks.	596,300
Training	Minimal training for Office of the CISO staff	5,000
Equipment	Support monitoring network for specific information security and privacy issues, development of new virtualization and reporting tools that provide situational awareness and intelligence for executives and their support staff, and support of new research opportunities for the campuses.	415,000
Total		$1,016,300

Option B – Fund the Office of the CISO budget to maintain a minimum due care approach for information security and privacy and produce self-assessment tools and services for UW colleges, school, and departments.

Description		Fiscal Year Expense
Salaries, wages, and benefits for 4 FTE	Develop a minimum set of resources that can be utilized by UW colleges, schools, and departments to develop their own strategies for addressing information security and privacy risks and threats.	469,000
Equipment	Minimal equipment necessary for staff to perform job duties.	25,000
Total		$494,000