University of Wisconsin–Madison
Campus Information Security Program
&
2018–2021 Cybersecurity Strategy

Executive Summary

December 31, 2018

Final

Endorsed by the UW-Madison Divisional Technology Advisory Group on December 21, 2018

Table of Contents

Record of Updates

Update Number	Change Information	Entered By	Date Entered
Final Draft for Release	Original document separated into an Executive Summary with an additional document containing detail of the Information Security Program and Cybersecurity Strategy. Formal review and endorsement by Divisional Technology Advisory Group on 12-21-2018	Bob Turner	**12/31/2018**

Executive Sponsor Review and Approval

Name	Role	Date
Lois Brooks	**Vice Provost for IT and CIO**	**01/07/2019**

Executive Stakeholder Review

Name	Role	Date
Joe Salmons	Chair, Information Technology Committee	
Laurent Heller	Vice Chancellor for Finance and Administration, University of Wisconsin-Madison	
Sarah Mangelsdorf	Provost, University of Wisconsin-Madison	

Related Documents

Document Name	Date
UW System Regent Policy Document 25-5, Information Security	**2/5/2016**
UW System Information Security Program v 1.0	**4/30/2018**

Executive Summary

The University of Wisconsin–Madison (UW-Madison) Information Security Program and Cybersecurity Strategy provides university executives and staff with a broad view of activities designed to protect information through collaboration, education, and innovation. UW-Madison seeks to optimize risk management by refining current useful strategies and goals and by defining new information security and cybersecurity strategies. The Program and Strategy is focused on protecting information in electronic, print and other formats with the scope being University-wide.

The Threat

During one week of 2018, the University encountered 121,499 vulnerability exploits to include brute-force and malicious code-execution. Of the events reported, 73 percent were of CRITICAL or HIGH severity. Cybersecurity risk management is complex as changes in security infrastructure, global criminal and nation-state threats, and the sophistication of exploits and volume of vulnerabilities continually increase. Also relevant are the continuing threats posed by criminal elements or nation-state actors who desire access to the volumes of data we hold.

The cybersecurity threat to UW-Madison information and our diverse but complex technology are real and increase or change monthly. Those threats include, but are not limited to:

- increasing compromise of campus credentials, likely as the result of phishing;
- user mistakes and errors;
- denial of service attacks;
- insider threats; and
- our inability to detect malicious code within encrypted communication paths.

The sophistication of phishing or other social engineering threats can easily lead to compromise of personal data or allow access to key information technology resources. Threat actors have increased the complexity of attacks directed at higher education. Cybersecurity industry reporting suggests increasing sophistication and changes to attack patterns in the categories of hacking, social engineering, and malware may include targeting of faculty and senior university leaders. Ransomware attacks carried out through website exploitation increase the likelihood that a major system or network outage could stop the business of the university with increased cost to recover.

Purpose and Use

The Information Security Program and Cybersecurity Strategy provides a framework for greater protection of data; management of the University's networks, information systems and applications; and the continued improvement to the people, processes, and technology that collectively execute the Program and enable continued success with the Strategy. The framework supports improving UW–Madison's cybersecurity posture.

For central and distributed information technology (IT) staff and security professionals, this program and strategy is an important guide to help them advance and sustain cybersecurity at UW-Madison. The document provides the readers with direction to sustain information systems in alignment with and in support of the University's mission. This Strategy incorporates feedback from the UW–Madison community based on lessons learned during implementation of the original 2015 Strategy. Information Security community representation in both the development and drafting teams along with IT and faculty governance review confirms this document has the support of the UW community,

reflecting greater cybersecurity maturity and evolving best practices that are easily integrated across the campus and transferrable to the University of Wisconsin System and other UW Institutions.

The accompanying Campus Information Security Program and 2018–2021 Cybersecurity Strategy document is the official description of the actions, activities and standards which shape information security at UW-Madison. Changes or exceptions to the program are to be submitted to the Office of Cybersecurity for processing, update, and subsequent approval by the Chief Information Officer. Deviations which cannot be effectively aligned to the UW System's information security program and supporting policies and standards will be submitted to the UW System Vice President for Information Security for review and concurrence.

All changes will be recorded with updates posted and announced per current communications policy, channels and standards.

Any exceptions to the UW System Information Security policies and associated standards should be evaluated based on the application to UW-Madison and the risk associated with the particular situation. This should include factors related to data classification, institutional objectives, regulatory and compliance matters, systems and processing criteria, and technology.

The Information Security Program

The Information Security Program is shown in Volume I of the Campus Information Security Program and 2018–2021 Cybersecurity Strategy document and supports the UW Board of Regents direction and the UW System Information Security Program. The mission, vision and guiding principles of the Program are specifically designed to support the UW–Madison missions of teaching, research and outreach.

As we continue to implement this program, we seek to perpetuate a culture at UW-Madison that values free and open exchange of ideas while respecting the need to keep information secure.

The UW–Madison Chief Information Security Officer and the Office of Cybersecurity are charged with creating and maintaining the initiatives that drive the Information Security Program forward. The fundamental cybersecurity tenets of availability, integrity, and confidentiality are applied to protect data and information technology assets from unauthorized access, loss, alteration, or damage. This supports the information sharing needs of academic and research environments while enabling the success of the administrative support and other campus business units.

Reducing cybersecurity risk while preserving information security is a shared goal and one of the primary areas of improvement for campus in the coming years. Risk reduction and management strategies address current threats. With the support of various campus advisory groups and governance bodies, cybersecurity must evolve to counter future threats and vulnerabilities in balance with the likelihood of exploitation.

The Cybersecurity Strategy

The elements of the Cybersecurity Strategy are contained in Volume II of the Campus Information Security Program and 2018–2021 Cybersecurity Strategy document. The elements are summarized below with Volume II containing specific and clearly defined SMART[1] goals. The strategic elements

[1] The SMART acronym first appeared in the November 1981 issue of Management Review. "There's a S.M.A.R.T. way to write management goals and objectives." written by George Doran, Arthur Miller, and James Cunningham.

are shown here:

- Strategy #1 – Community: *Build a community of experts to improve institutional user competence through Security Education, Training, and Awareness.*

The types of activities supporting this strategy may include continued evolution of the awareness and educational aspects of the program; annually measuring the state of cybersecurity awareness; and development of Cybersecurity Risk Management training.

- Strategy #2 – Service Alignment: *Build and align cybersecurity services used by the Office of Cybersecurity and distributed IT service providers to gain efficiencies for UW–Madison and UW System by utilizing common best practices.*

The types of activities supporting this strategy may include performing annual reviews of campus cybersecurity services; creating a cybersecurity governance oversight process; and identifying common best practice approaches for existing services while identifying gaps or redundancies in service operations.

- Strategy #3 – *Measure: Establish security metrics, optimize services, promote compliance, achieve Continuous Diagnostics and Mitigation (CDM).*

The types of activities supporting this strategy may include establishing and implementing a framework for CDM; understanding and improving the use of cybersecurity tools; and continually enhancing the Cybersecurity Risk Management Program.

- Strategy #4 – Data: *Develop processes that aid end-users and organizations in managing data throughout its lifecycle, including provision of services that support data inventory, classification, and protection as defined in Risk Management Framework.*

The types of activities supporting this strategy may include developing templates of ready-to-implement security controls, safeguards or countermeasures along with efforts to promote and encourage the development of cost-effective restricted data storage services.

- Strategy #5 – Trust: *Improve relationships that advance trust through understanding among local and distributed IT organizations, service providers, and the Office of Cybersecurity. This includes jointly developing sustainable security services that are respectful to academic freedom and personal privacy, with well-defined frameworks and processes that allow close collaboration between campus stakeholders and the Office of Cybersecurity.*

The types of activities supporting this strategy may include developing activities and projects that clearly demonstrate to campus stakeholders an enduring respect for academic freedom and personal privacy in cybersecurity operations by leveraging internal and external marketing expertise.

- Strategy #6 – *Operational Risk: Establish a centralized process to detect and mitigate threats, disseminate threat intelligence, and improve those capabilities for stakeholders.*

The types of activities supporting this strategy may include further evolution of the Cybersecurity Operations Center (CSOC) to detect and analyze threats with due consideration to expansion of service to 24-hour operations.

- Strategy #7 – *Research and Outreach: Partner with stakeholders at the University to be the champion for educational experiences, student jobs, internships, research and public activities, risk management and analysis, privacy, and identity management, thereby becoming a model organization for other cybersecurity teams throughout Wisconsin.*

The types of activities supporting this strategy may include additional partnerships with faculty and researchers; support of students with interest in cybersecurity through internships and additional training opportunities; and direct involvement with research that develops new security controls.

Intended Outcomes

By adhering to the Information Security Program and executing the strategies above, we will measurably improve institutional user competence, more effectively manage risk, and provide a return on the investments made over the last three years and into the future.

Challenges and Areas for Improvement

Centralized and distributed levels of IT and security must confront several challenges and areas for improvement. These include:

- the distributed nature of the University communities is a strength, as it keeps the IT professionals right next to the supported academic, research, and outreach projects. It also presents challenges with coordination, communications, and consistency in interpreting IT and cybersecurity standards, practices, and guidelines;
- diverse and changing technology, business processes, use cases, and cybersecurity skill levels;
- the need for defined and consistent cybersecurity services that establish responsibilities for managing and leveraging the centralized and distributed IT and cybersecurity professionals;
- different and competing priorities compounded by the ever-changing nature of security laws, policies, and procedures;
- the recruitment and sustainability of a diverse and highly skilled cybersecurity workforce; and
- the need for consistent sources of renewable funding and alignment of funding to the needs of central, distributed, and UW System IT service providers, system owners, and data stewards.

Primary areas for improvement are found in risk reduction, including threat detection and mitigation; and in the accurate classification and protection of data.

Contact

The point of contact for information or questions regarding the UW-Madison Information Security Program and Cybersecurity Strategy is the Chief Information Security Officer. Additional information and subsequent updates to the program and strategy are available on the Office of Cybersecurity website at https://it.wisc.edu/about/office-of-the-cio/cybersecurity/