IT STRATEGY BOARD

May 5, 2015

INFORMATION TECHNOLOGY

UNIVERSITY *of* WASHINGTON

AGENDA

- Call to Order
- HR/P Modernization Update
- University Information Security and Privacy Strategy and Initiatives
- IT Project Portfolio Executive Review
- Wrap up

HR/P Modernization Update

Cheryl Scott
Assistant Vice President, HR Payroll Modernization Project

Decision to Continue Semi-Monthly Pay Frequency in Workday

> Initial decision to move to a biweekly pay cycle
  - —Semi-monthly configuration did not meet our compliance needs
  - —Biweekly provided efficiencies and reporting of benefit to UWMC and HMC

> Challenges associated with a biweekly pay cycle were raised that we are not able to resolve
  - —Complexities in UW's pay practices
  - —Challenges with monthly financial reporting
  - —Cumbersome workarounds to meet DRS reporting requirements

> Sponsors made the decision to retain a semi-monthly pay frequency

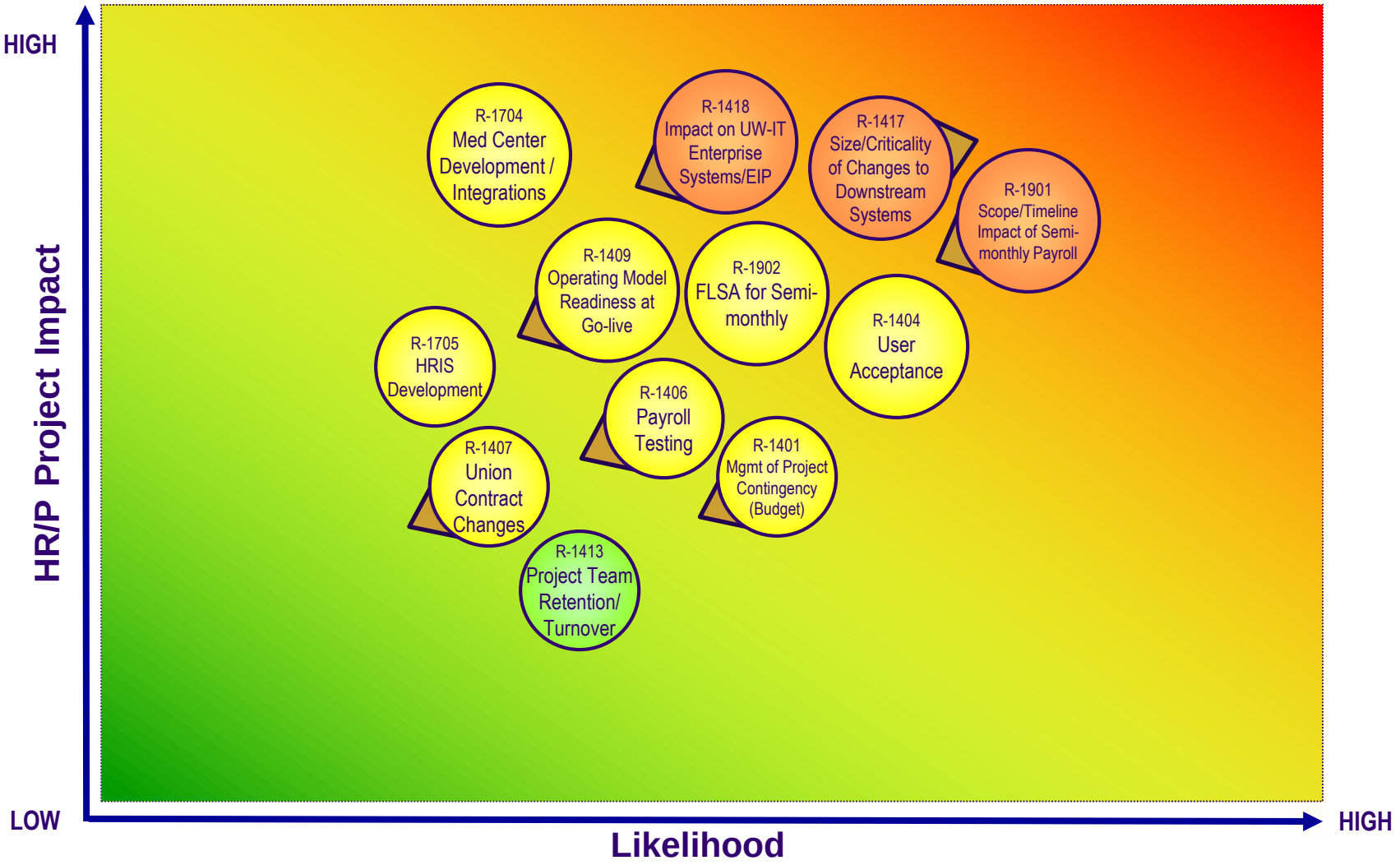
HR/P: A Transformative Opportunity

HR/Payroll Modernization will:

- Improve critical HR and payroll practices
- Strengthen regulatory compliance
- Deliver better information for decision making
- Produce substantial efficiencies and productivity gains throughout all UW units

By updating our HR and payroll processes and the underlying system that supports those processes, UW will reduce risk, increase efficiency, and operate more effectively as a world-class institution.

HR/P Key Risks – April 2015



Legend

- Bubble size indicates impact
- Project impact relates to impact on HR/P project
- Bubble color indicates risk severity (a combination of project & schedule impact and likelihood)
- Arrow shows directional change since last report

HR/P Key Risks – April 2015

Risk #	Risk	Mitigation Plan
R-1401	Management of the project contingency (budget)	Monitor project plan, schedule and budget impacts from semi-monthly payroll cycle change
R-1404	User Acceptance	Developing a comprehensive change management plan to ensure impacted users are trained on new processes and systems prior to go-live; executing on a comprehensive communications plan
R-1406	Payroll Testing Complexities	Developing a comprehensive plan for payroll parallel testing; adding a Test Coordinator dedicated to payroll testing (simpler given the change to semi-monthly payroll); preparing to test the payroll comparison tool
R-1407	Union Contract Negotiations / Changes to Union Contracts	Staying in close contact with Labor Relations, HR and Medical Centers to understand progress on union negotiations
R-1409	Operating (Support) Model Readiness at Go-live	Developing conceptual design of support organization early in the project; ensure team is staffed and trained prior to go-live
R-1413	Project Team Retention / Turnover	PMO regularly assesses resource risks; using contractor / other resources to fill gap while resources are hired; reviewing market salary data for similar positions; managing turnover of HEPPS Production Support team
R-1417	Size / Criticality of Changes to Downstream Systems	Work with UW-IT and HRP-Intersections team to scope this work; monitor key milestones
R-1418	Impact on UW-IT Enterprise Systems / EIP	HRP-M and HRP-Intersections are working closely together to scope the work, ensure adequate resourcing and monitor key milestones; joint status reporting weekly
R-1704	Medical Center Development / Integrations (interdependent project)	HRP-M and Medical Centers are working closely together to scope the work, ensure adequate resourcing and monitor key milestones
R-1705	HRIS Development (interdependent project)	HRP-M and HRIS are working closely together to scope the work, ensure adequate resourcing and monitor key milestones
R-1901	Scope and Timeline Impacts of Moving to Semi-monthly Payroll	Impact assessment of change to semi-monthly payroll has been completed; making changes to designs and configuration
R-1902	FLSA Functionality in Workday for Semi-monthly Payroll	Participating in Workday work group to define functionality for FLSA semi-monthly; targeted to be released in September 2015 (Workday 25)

Risks Mitigated

The decision to remain on semi-monthly pay substantially reduces some of the project's highest risks, including:

- Reduces integrations work with mainframe, data warehouses and downstream systems
- Improves user acceptance by reducing the change impacts

Configuration and Prototype Phase Work (through July 10, 2015)

- Focused on building the system that was designed during the Design Phase
  - Loading P1 and P2 data (very comprehensive data)
  - Ensuring functional processes work
  - Completing end-to-end business process documentation
  - Building and testing integrations, and collecting new report requirements
  - Developing test plans and scripts for the test phase
- Increasing unit engagement
  - Conducting unit-specific impact assessment
  - Developing readiness teams
  - Increasing communications
  - Preparing training strategy and training materials

New User-Friendly URL

MyWorkday.uw.edu

hrpmod@uw.edu

HR/Payroll
MODERNIZATION

UNIVERSITY of WASHINGTON

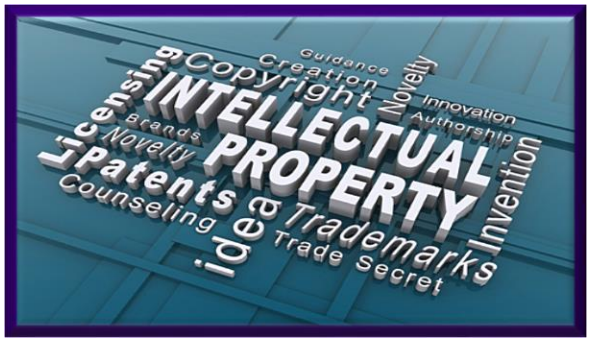
University Information Security and Privacy Strategy and Initiatives

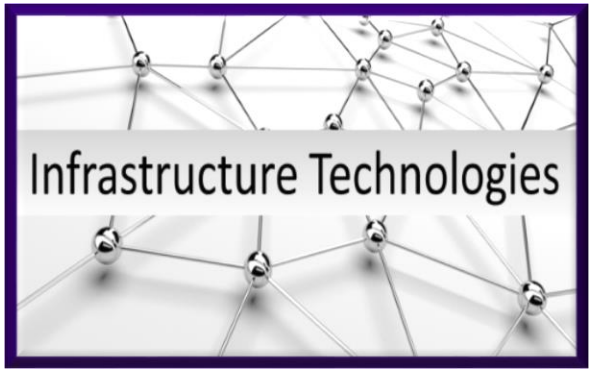
Kirk Bailey
Associate Vice President and Chief Information Security Officer

Ann Nagel
Associate Chief Information Security Officer

The Office of the CISO

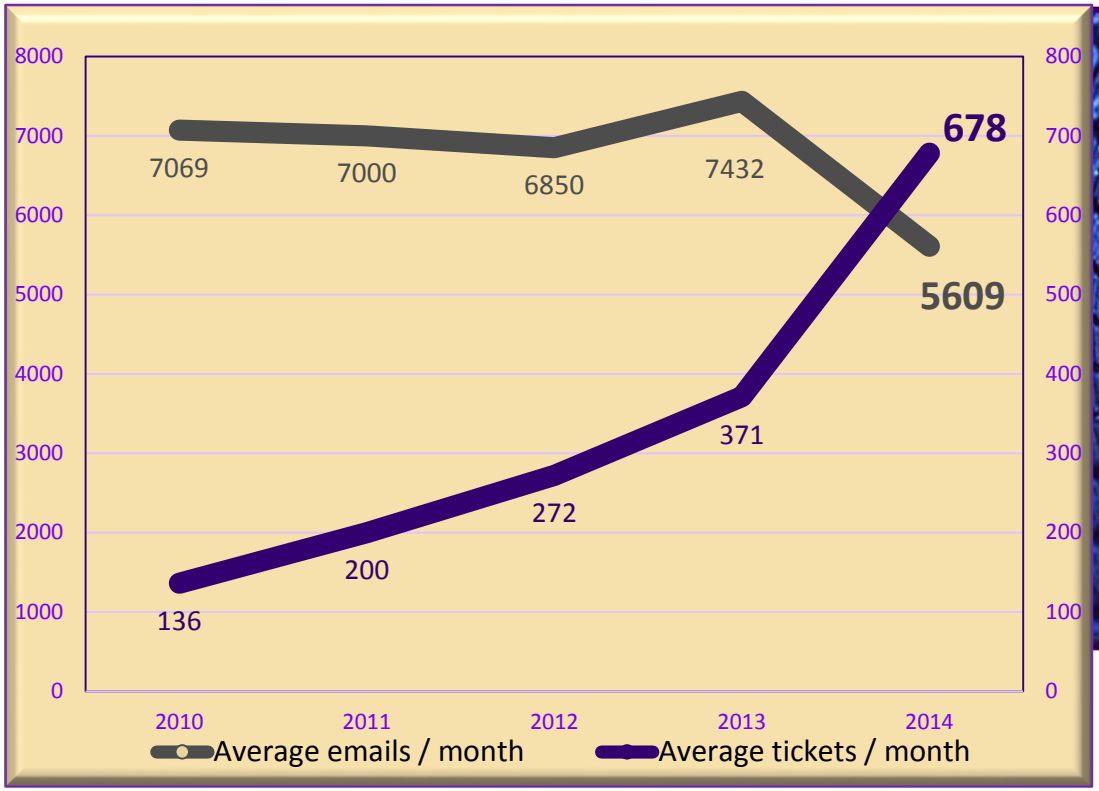
Cyber-based Security Risks @ UW



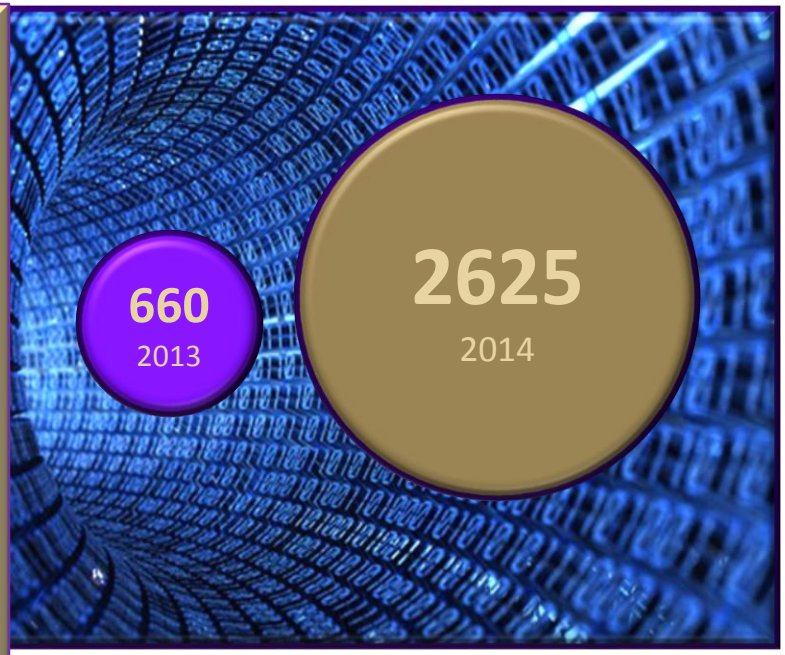


ON THE FrontLines

Email & Ticket Trends



Compromised NetIDs disabled



Stress Reduction by Wise Strategy

Strategy

- Smart and pragmatic risk management practices
- Optimizes finite resources to mitigate risk around University academic and administrative areas
- Focuses on critical assets and related threat landscape
- Provides reliable counsel and support based on in-depth situational awareness

The OFFICE OF THE CISO

- Home

- About Us
- Annual Reports
- CISO Newsletter
- Events
- Frequently Asked Questions
- Information Security and Privacy Laws and Regulations
- **Information Security and Privacy Risk Management**
- PASS Council
- Report an Information Security or Privacy Incident
- Resources
- Services
- UW Privacy Program

Search for:

Information Security and Privacy Risk Management

Academic and research institutions offer a uniquely attractive target for cyber criminals. These institutions typically have a considerable number of user login credentials that can be stolen to access valuable research data, intellectual property, library resources, and stores of personal information that are potentially exploitable for identity theft.

Below is a suite of resources for understanding and managing security and privacy risks at UW.

Check this webpage frequently to make sure you are using the most recent version of risk management resources. The resources will continuously evolve as new ones are released.

Develop a Security Plan

- Develop an Approach
- Identify Information Assets
- Assess Risk
- Create a Strategy

Document Data Sharing Relationships

- Document Data Flow
- Interdepartmental Data Sharing
- External Data Sharing

Request Help

http://ciso.washington.edu/

Are We Heading the Right Direction?

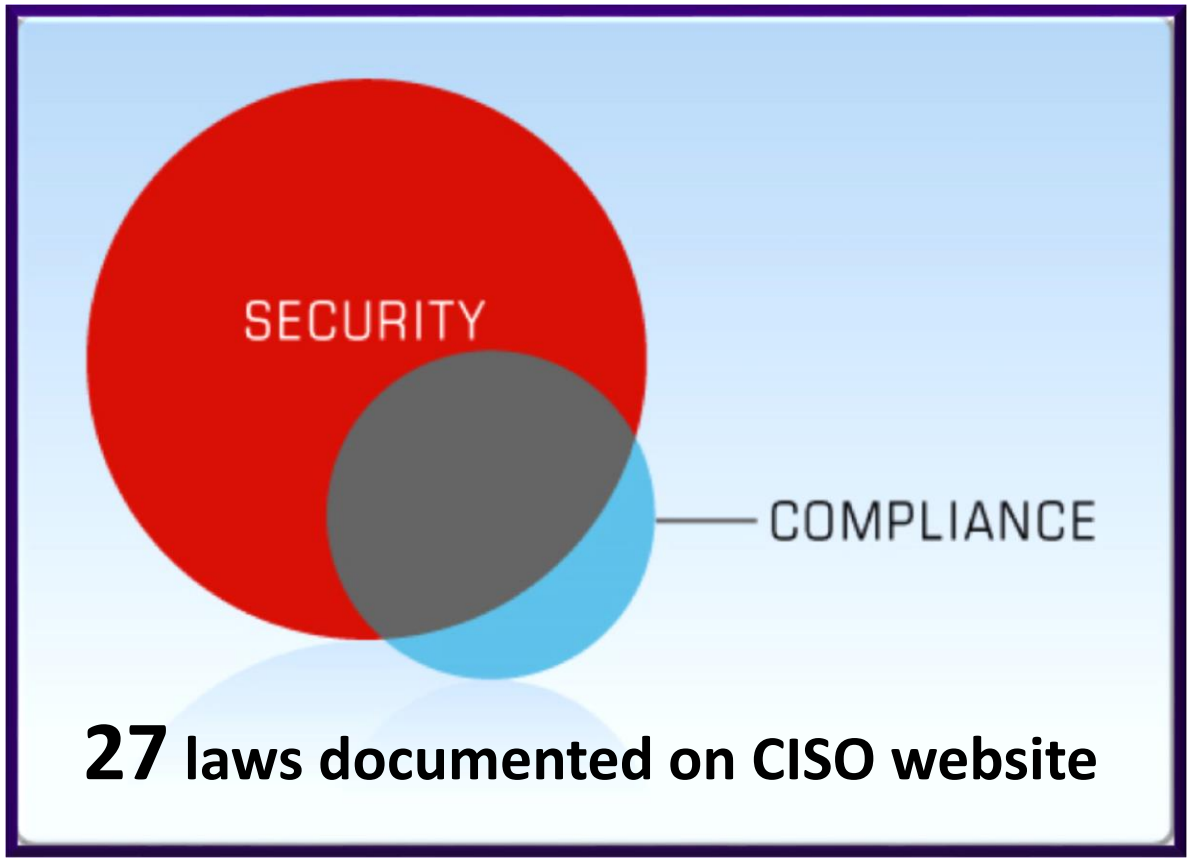
Key Program Elements

- Strong and established governance for privacy and information security
- Emerging threat intelligence practices
- Innovative situational awareness practices for intelligence analysis and risk management decisions
- Mature incident response and management capability
- Targeted and appropriate risk transfer terms

Key Program Elements

- Thoughtfully developed and maintained industry contacts
- Access to non-public information sharing resources
- Essential and balanced institutional policies
- Relevant training and awareness activities and online resources
- Intellectually diverse and innovative staff

Compliance is Not Security



SUPPORT FOR “DUE CARE” APPROACH

Office of CISO Staff

- Total of 15 full-time positions
- Staff professional credentials include:
  - Certified Information Security Professional (CISSP) – 7
  - Certified Information Security Manager (CISM) – 2
  - Certified Information Security Auditor (CISA) – 1
  - Certified Information Privacy Professional (CIPP/US) – 1
  - Cyber Security Forensic Analyst (CSFA) – 5
  - Certified Ethical Hacker (CEH) – 3
- Staff skills and experience include:
  - Training development
  - Cybersecurity and privacy compliance programs
  - Consulting, audit practices, and risk management
  - Technical, architecture, and development expertise
  - Threat intelligence analysis skills

HIGH DEMAND FOR TALENT

Questions

IT Project Portfolio Executive Review

QUESTIONS AND DISCUSSION