



Security Professionals Conference 2018
Security and Privacy Professionals:
“All Hands on Deck”

***Promoting Enterprise Risk Management (ERM) and
Governance, Risk and Compliance (GRC) for
Managing Cybersecurity Risks***

Peter J. Murray, PhD
Chief Information Officer and
Vice President for Information Technology

Roger J. Ward, EdD, JD, MPA
Senior Vice President for Operations and Institutional Effectiveness and
Vice Dean of the Graduate School



This presentation leaves copyright of the content to the presenter. Unless otherwise noted in the materials, uploaded content carries the [Creative Commons Attribution-NonCommercial-ShareAlike license](#), which grants usage to the general public with the stipulated criteria.



Who We Are and What We Do

Dr. Roger J. Ward



Senior Vice President for Operations and Institutional Effectiveness and Vice Dean of the Graduate School

ERM, Accountability, Compliance

Dr. Peter J. Murray



Chief Information Officer and Vice President for Information Technology

IT GRC, IT Security & Compliance



Presentation Roadmap

- About UMB
- Scope and scale of cybersecurity threat
- Enterprise approach to managing the cybersecurity threat
- Enterprise Risk Management (ERM)
- Governance, Risk, and Compliance Framework (GRC)
- Lessons learned
- Takeaways



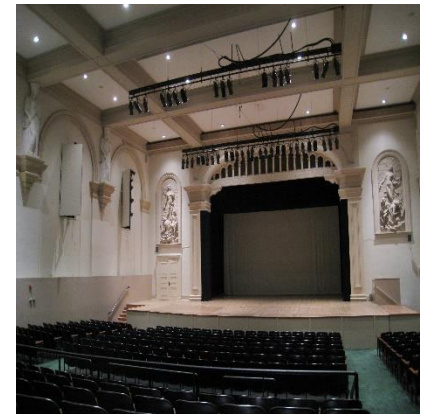
UNIVERSITY of MARYLAND
BALTIMORE



OriolesTM

*The official travel website for
Baltimore:*

<http://baltimore.org/>





About UMB

- **UMB** is the founding campus (1807) of the University System of Maryland
- **Mission:** To improve the human condition and serve the public good of Maryland and society at-large through education, research, clinical care and service
- **Schools:** Dentistry, Graduate, Law, Medicine, Nursing, Pharmacy & Social Work
- **Students:** 6,703
 - Graduate and Professional: 86%
 - Undergraduate: 14%
 - Full-time: 77%; Part-time: 23%
- **Employees** (includes faculty): 7,360
 - Full-time: 71%; Part-time: 29%
 - Faculty: 2,839
- **Annual Budget:** ~\$1B
- **Grants and Contracts:** ~\$556k





UNIVERSITY of MARYLAND
BALTIMORE

***An Academic Health, Law and Human Services University
Education, Research and Patient Care***



**Protected Health Information
Personally Identifiable Information
Confidential Research, Business and Academic Data**

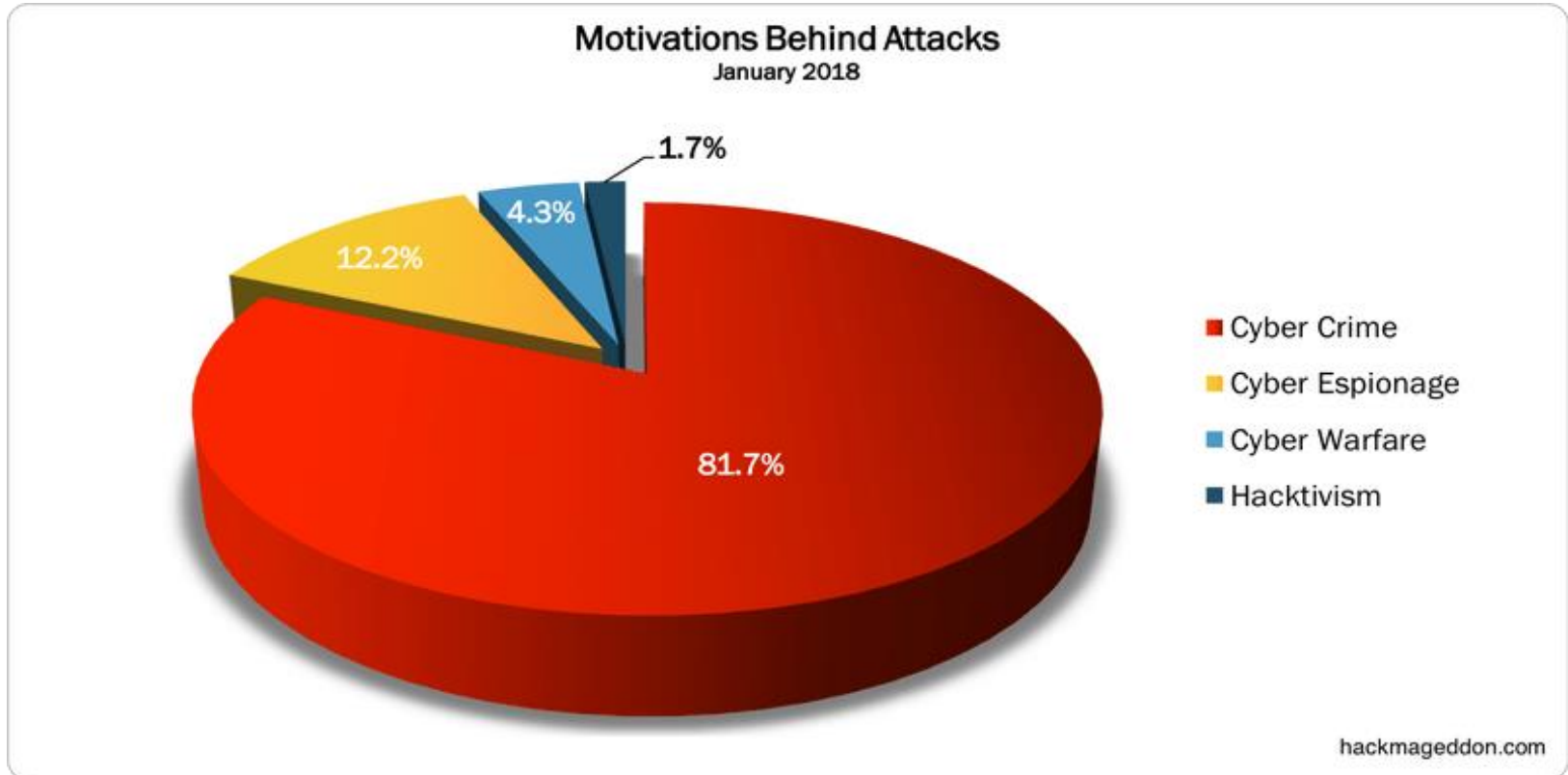


So Why Are We Giving This Presentation



What it Means to the University

- It is critically important to us; an institutional priority
- It is strategic to the institution since it affects all of the missions of the institution: Education, Research, Clinical Care
- It is a key element in our IT GRC and ERM programs
- It is not "just another worry," one area (out of many) that we are ultimately responsible for managing



- Cyber crime damage costs to hit \$6 trillion annually by 2021¹
- The average cost of a data breach for US companies is \$217 for each compromised record (\$225 for higher education) and the total average cost is \$6.5 million²

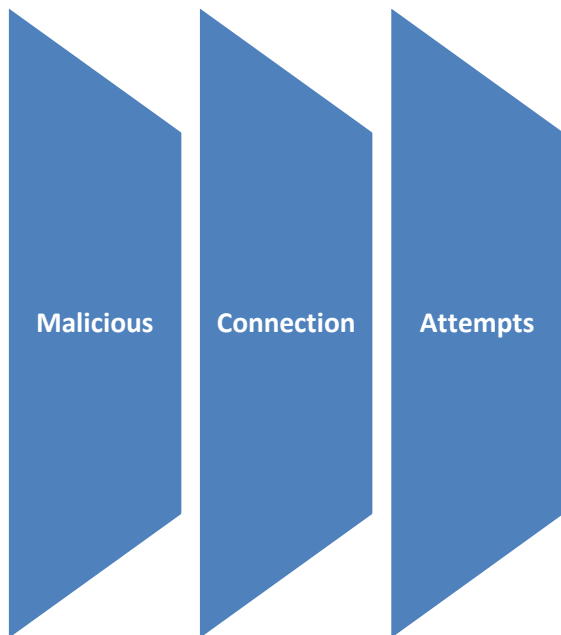
¹ Steve Morgan, CSO from IDG, Cybersecurity Business Report, *Top 5 Cybersecurity facts, figures and statistics for 2018*, January 2018

² Ponemon Institute Research Report, *2015 Cost of Data Breach Study: United States*, May 2015

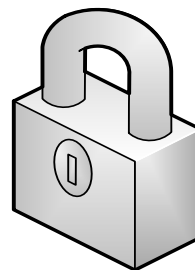


Evolution of the Cyber Security and Threat Environment

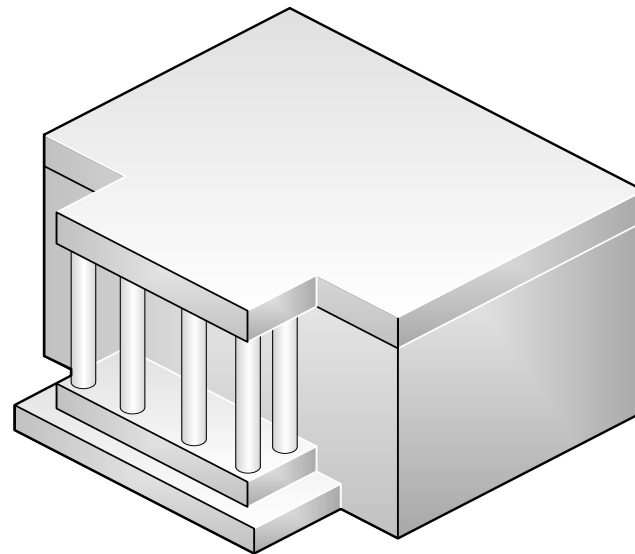
INTRUSION DETECTION AND PREVENTION



Over 20 Million Per Day!!!



**UMB
Intrusion
Detection/
Prevention
System**

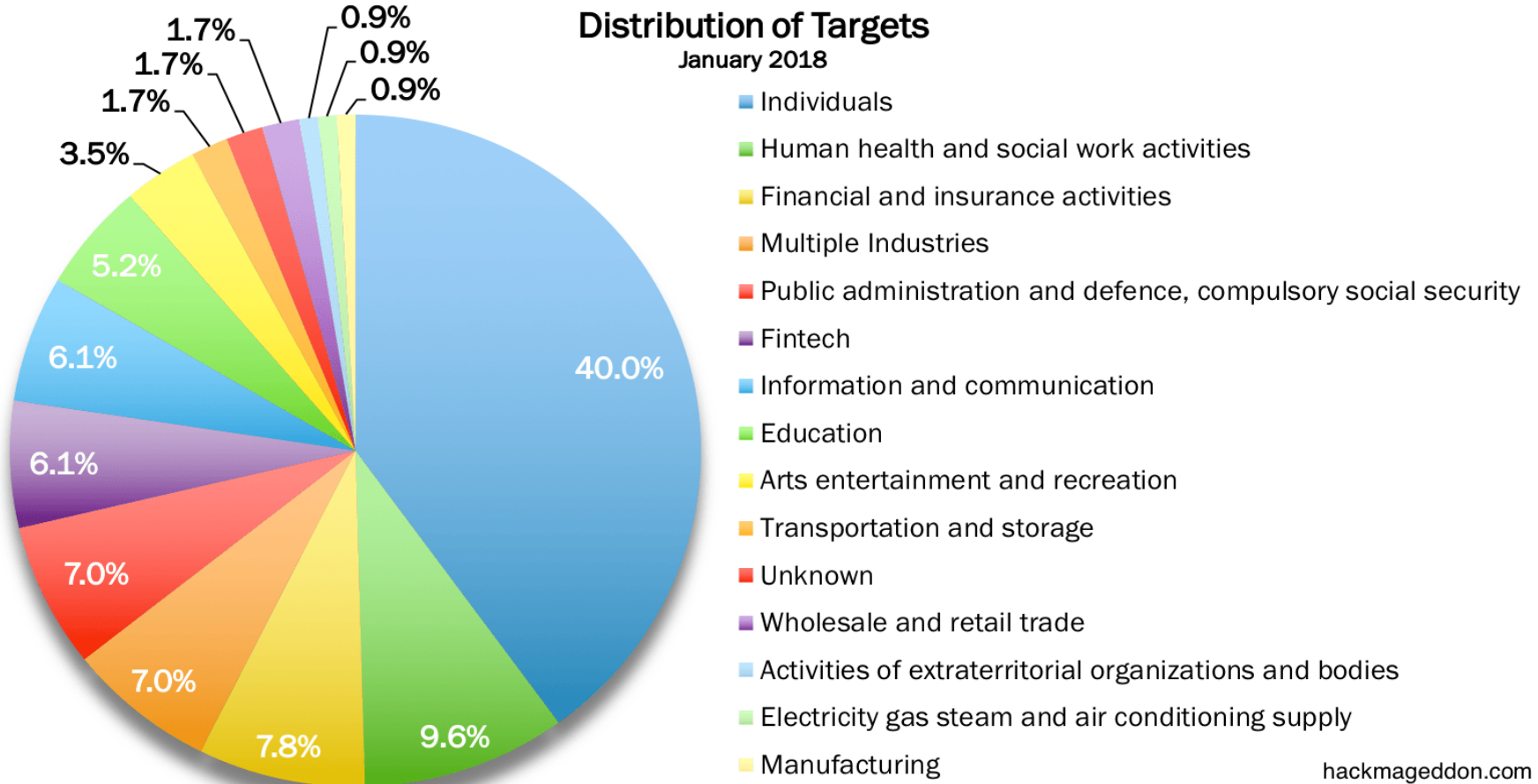


**Blocked at Our Network
Gateway to the Internet**



Distribution of Targets

January 2018



hackmageddon.com

Single individuals lead with 40%!



Raising Awareness of Basic Cybersecurity Hygiene



- Malicious emails
- Email phishing, malware
- Incoming email, 20% “clean”
- Individuals are targets!!



- Nearly 1/3 of breaches are the result of “unintentional disclosure”¹
- Preventable!!



Potential Impact of Cyber Attacks

Reputation

- May harm the University's reputation in the eyes of alumni, students, partners, businesses, and government agencies

Legal

- May leave the University in violation of laws or contract requirements
- Risk of prosecution, financial penalties, or withdrawal of existing and future funding

Economic

- May undermine the University's ability to capitalize on potential intellectual property or knowledge transfer

Operational

- May disrupt normal operations and result in significant remedial cost



Cybersecurity and Compliance



- **Overwhelming amount of work for IT security staff to manage risks, identify threats, prevent attacks, address vulnerabilities, and protect data assets**
- **Cybersecurity requires “all hands on deck”, including individuals from all areas and levels of the University**



GRC and ERM Frameworks

Governance, Risk, and Compliance Framework

- A structure that an institution uses for governance, risk and compliance initiatives
- A means for establishing governance, identifying and assessing risks, and achieving compliance
- Integrated, collaborative approach for producing desired results. It breaks down silos so that a single united solution can be implemented



Enterprise, Risk, Management Framework

- A method and process for minimizing unexpected volatility through the assessment of risks across every function
- Includes identifying and evaluating risks, and developing mitigation strategies
- Shares the same end goal as GRC: the continued achievement of the institution's goals and objectives





Enterprise Risk Management (ERM)

- A **RISK** is any issue that impacts an organization's ability to meet its objectives
- **ERM** is a senior leadership driven initiative that seeks to integrate risk management practices throughout the organization in order to address uncertainty and risk while enhancing the ability to achieve organizational objectives (COSO, 2004, p. 16; Hoyt & Liebenberg, 2003, p. 37)



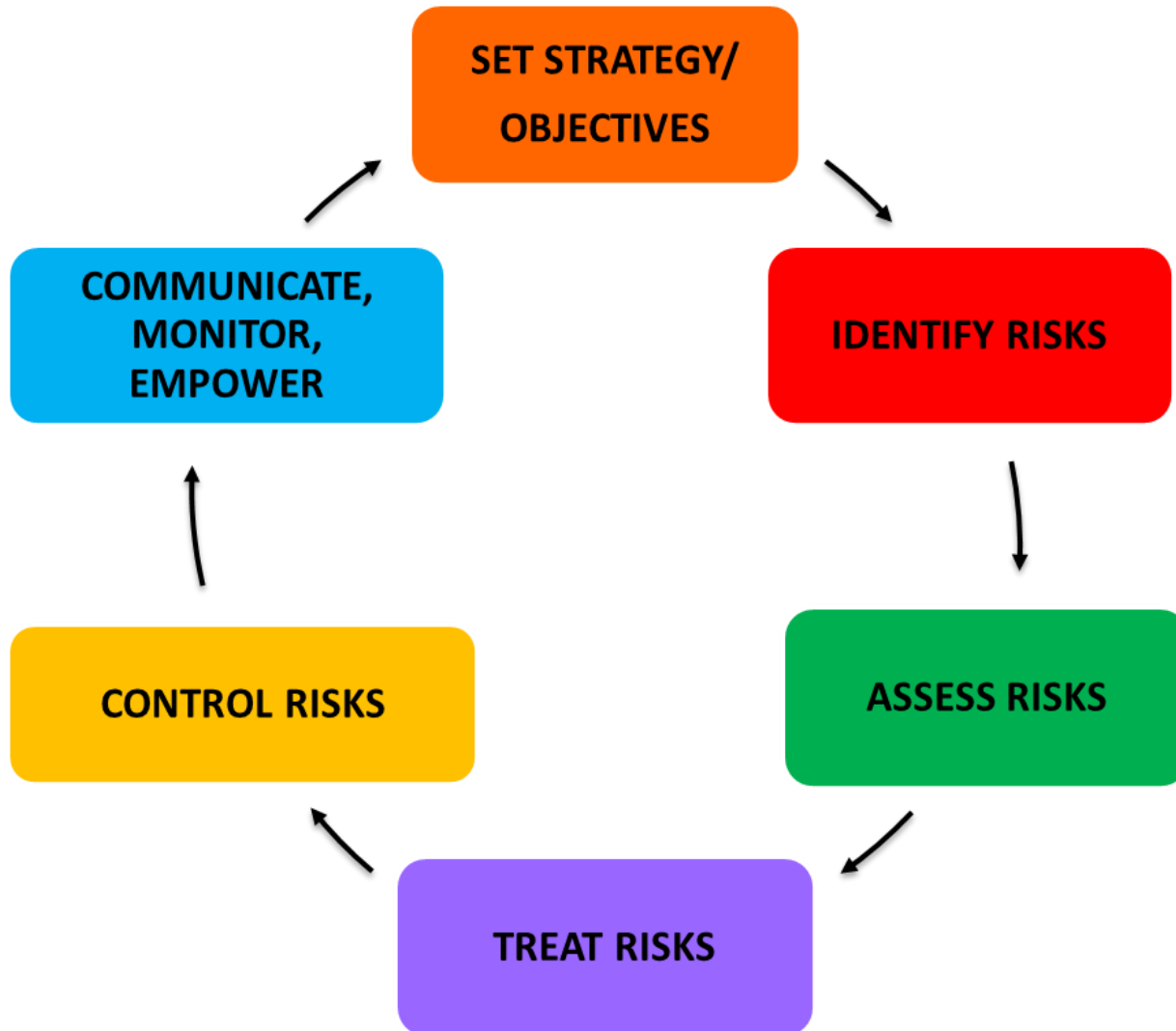


Enterprise Risk Management (ERM)

- It is a process initiated and effected by an organization's leadership
- Developed and managed at the 'enterprise' as opposed to the unit or operational level
- Designed to identify and mitigate risks that would impact strategic objectives, and
- Provides a framework for determining risk tolerance, developing mitigating strategies, and allocating resources



The ERM Cycle





The Benefits of ERM

1. Improves management of known risks that may prevent the organization from accomplishing its mission and goals
2. Reduces duplication of effort on key activities across operational units
3. Enhances the coordination of activities and communication across operational units
4. Improves regulatory compliance
5. Reduces operational losses and surprises
6. Integrates risk management with business planning and strategy setting
7. Protects reputation and brand
8. Creates a risk aware culture



IT GRC Framework

- **Governance, Risk, and Compliance (GRC) Framework:**
 - A framework for the leadership, organization, and operation of the institution's IT areas to ensure that those areas support and enable the institution's strategic objectives. (Joanna Grama and Rodney Peterson)¹



- IT GRC programs align institutional activities with larger institutional goals (i.e., governance) and allow the identification of challenges and opportunities (i.e., risk), and when internal requirements and external mandates are lined up (i.e., compliance), institutional activities have the best chance for success—especially in stormy weather or where danger lurks. (Diana Oblinger)¹



IT GRC in Higher Education

Governance



81% of institutions do not include IT risk in their institution's strategic plan. While information security was ranked the highest by institutions as an IT risk, there was a gap between its importance and the effectiveness in addressing this IT risk¹

Only 56% of all H.E. institutions have IT governance in place¹

COMPLIANCE



Only 2 out of 5 institutions indicate that they have a process for reviewing IT compliance practices, and only 1 out of 5 indicate that they have an adequate budget devoted to IT compliance¹

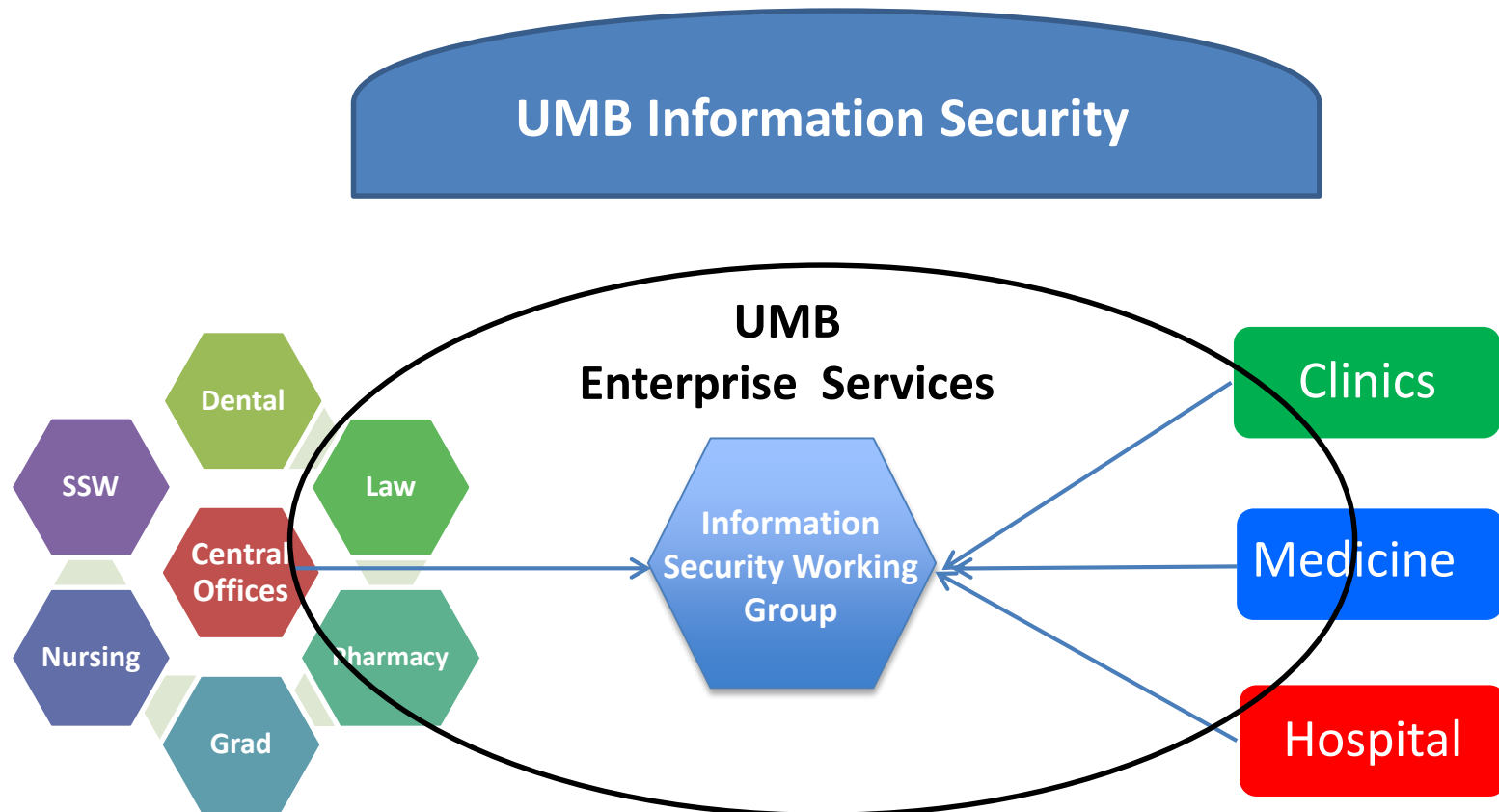


IT GRC and Cybersecurity at UMB

Cybersecurity Collaborative

- A multi-organizational structure facilitates information sharing and coordination of effort between schools, departments, clinics, and the hospital
- Aligned with the institution's strategic plan and a key area in the institution's enterprise risk management program
- An integrated and collaborative governance model has been established that includes an executive committee and an IT Leaders group
- An Information Security Working Group identifies information security risks, and works collaboratively to address IT security compliance with internal requirements and external mandates that include audit requirements, laws and regulations

IT GRC and Cybersecurity at UMB Enterprise Model: Cybersecurity Collaborative



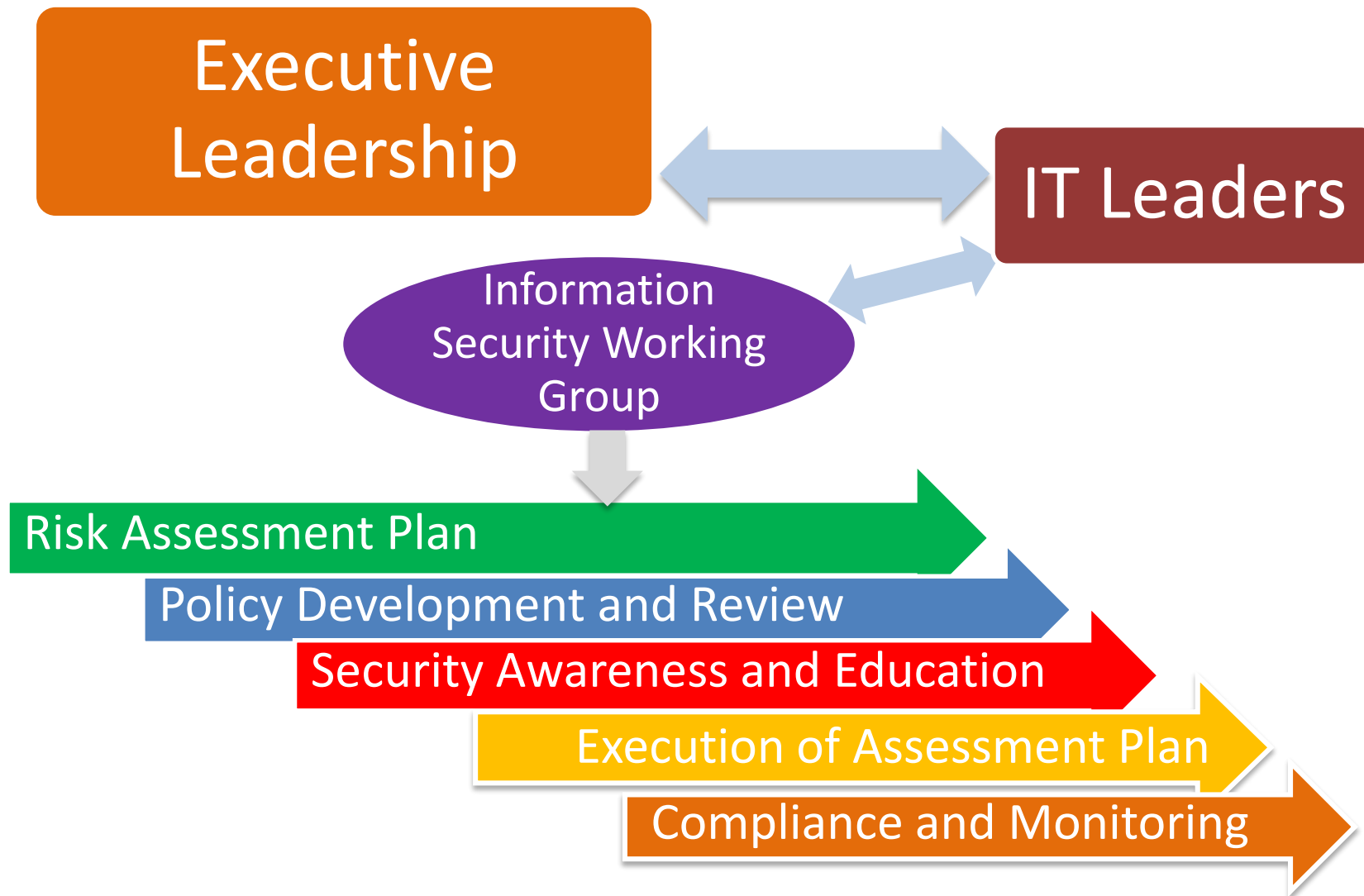


Primary Objectives of the Cybersecurity Collaborative

- Identify, assess, and report on any information security risk or vulnerability
- Define common areas of risk as they relate to information security at appropriate operational intersections
- Share effective information security strategies
- Share technology solutions and technical knowledge
- Collaborate on the improvement and enforcement of information security policies
- Develop a global communication strategy to promote and expand information security awareness
- Collaborate on the improvement and strengthening of information security policies, practices, and solutions, and ensure coverage and compliance across the enterprise



GRC Cybersecurity Framework at UMB





Success Indicators: Two Reasons Why the UMB GRC Cybersecurity Framework is Working So Well

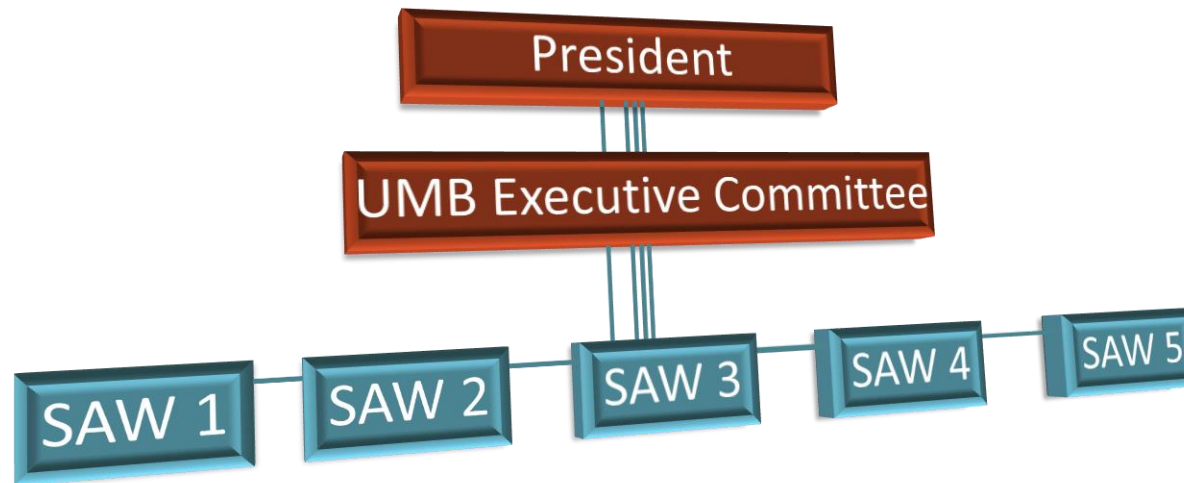
- We are taking an enterprise approach to information security, which means active participation, resource commitment and prioritization by each area represented in the cybersecurity collaborative

And,

- It is not just an activity that we are working on as time permits or in response to an event. It has become an integral part of the UMB culture, UMB Strategic Plan, the ERM program, and academic and business processes



UMB IT GRC and ERM Experience Our Principles and Approach



- Collaboration across the enterprise
- Added visibility and value to IT Security



UMB IT GRC and ERM Experience

What We Have Learned

- First cycle will identify mostly operational risks
- Leadership must make a conscious effort to identify strategic risks
- Strategic plan may provide a useful framework for evaluating risks and determining priority
- The ERM process is just as important as the product
- Sustaining funding for the program is a challenge
- It's a process not a project
- Must be mindful of process fatigue; affects leaders more than participants
- And influences an important positive change as the institution moves from IT Security GRC to an enterprise program of governance, risk, management and compliance



Value of Using GRC and ERM Frameworks

- The ERM program and structure at the University of Maryland Baltimore:
 - Adds visibility and value to the Cybersecurity program
 - Facilitates communication and collaboration across the enterprise
 - Changes the culture to be more Cybersecurity aware
- Cybersecurity can't be addressed in silos, and just by the IT organization
- Cybersecurity is only as strong as the weakest link in the institution
- Using GRC and ERM frameworks make it an enterprise-wide program
- It has to be viewed as an enterprise issue since it impacts all missions of the institution



If You Don't Have a GRC and ERM Program at Your Institution...

Some key things you can do:

- Keep reminding institutional leadership of the potential impact of not addressing cybersecurity risks...keep the risks visible and in the forefront
- Use Educause and other resources to point out what can happen, and what has happened, at other institutions when risks aren't addressed
- Take advantage of the public consciousness regarding Cybersecurity and the constant news of organizations experiencing breaches
- Tie the message to how unattended risks at your institution could lead to a breach that would impact the reputation, finances, legal aspects as well as the operations of the institution



Educause Resources

IT Governance

- IT Governance Toolkit
- Higher Education IT Governance Checklist
- IT Governance, Risk, and Compliance in Higher Education

IT Risk Management

- Thinking about IT Risk Strategically
- IT Risk Register
- Understanding IT GRC in Higher Education: IT Risk
- Risk Management Basics

IT Compliance

- Understanding IT GRC in Higher Education: IT Risk
- Higher Education Compliance Matrix
- New Federal Data Protection Requirements Impact Higher Education Institutions



Presentation Take-Aways

- Cybersecurity is an enterprise-wide issue and activity
- Strengthened by GRC and ERM frameworks and programs
- It needs to be aligned with the institutional strategic plan, goals and objectives
- Cybersecurity awareness across the institutional community will help change the culture and be an issue that all levels of the institution will appreciate
- It requires engaging your community and communicating to anybody and everybody that cybersecurity is a strategic risk and requires “All Hands on Deck” for an information security program to be successful



UNIVERSITY *of* MARYLAND
BALTIMORE

Questions?