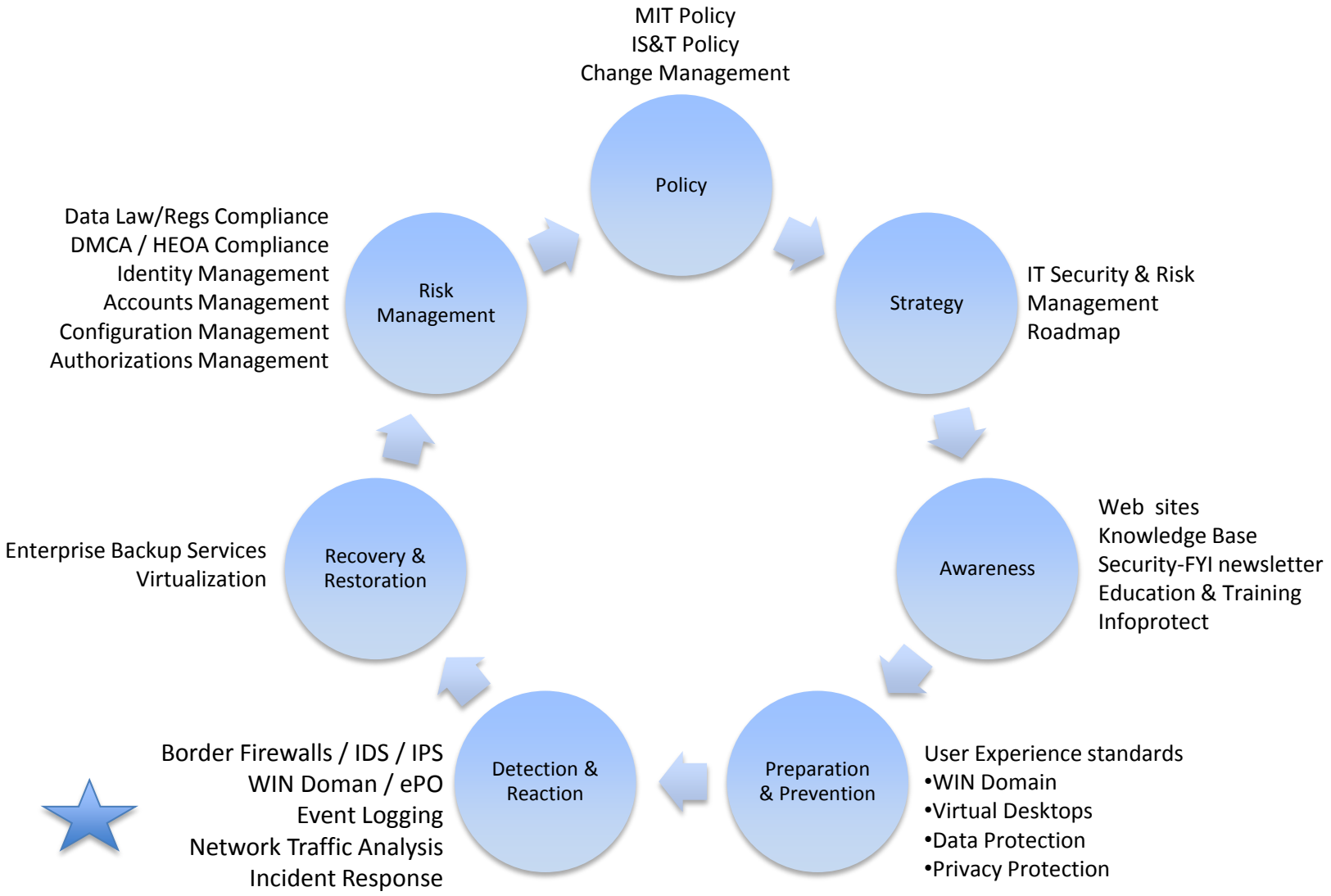
Network Security Roadmap

February 15, 2011

The IT Security landscape

Many Dimensions of IT Security

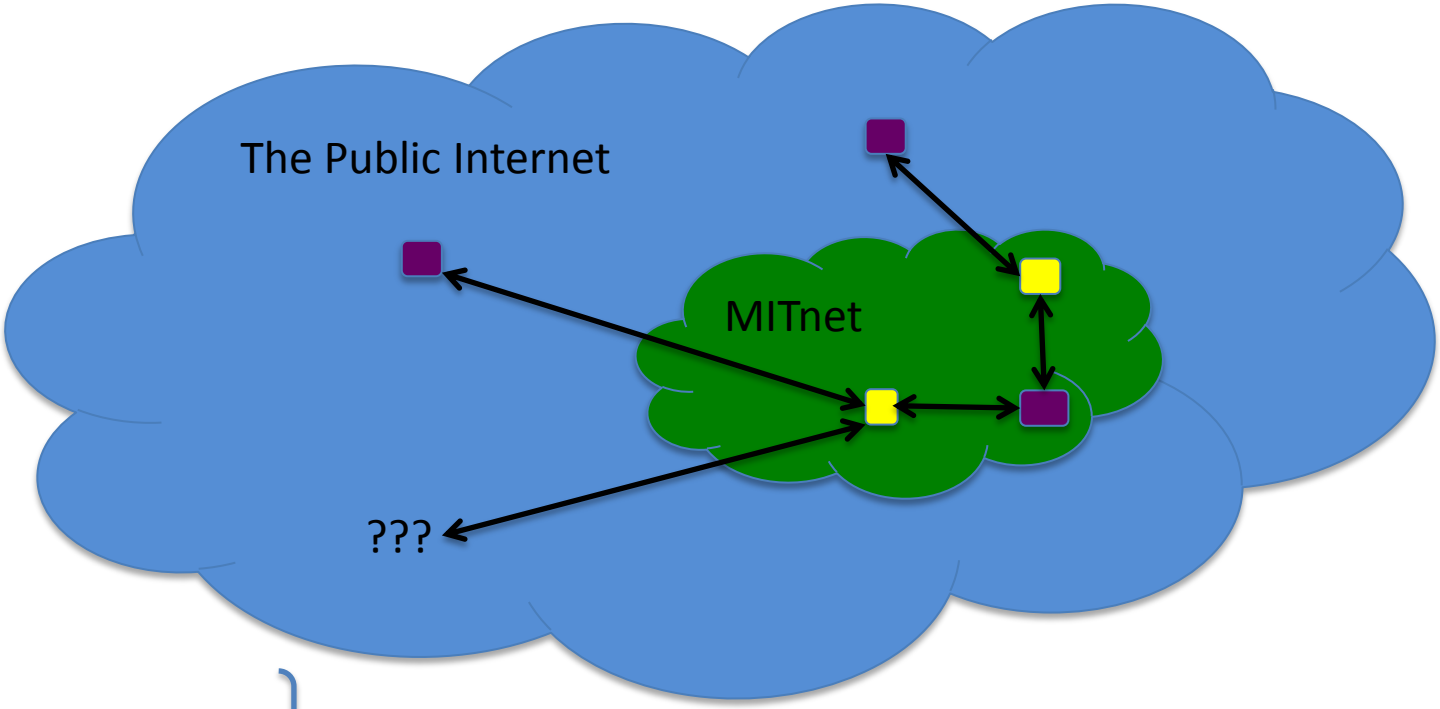


Current Challenges

- IT Security approach today is reactive, one-off, labor intensive and lacking useful data
- Most incident detection re: MIT computers comes from 3rd parties
- We have sparse data on MITnet's uses
- Computers are not adequately protected from attack – from both inside and outside
- Compromises reduce productivity, put sensitive data and IP at risk, and lead to legal, financial and reputational harm

Traditional View

The Public Internet is wonderful, we should do everything possible to ENABLE computers on MITnet to access anything and everything on the Public Internet, and vice versa, and to think of MIT and MITnet as if they were simply a subset of the Public Internet, particularly from a policy point of view.



Examples

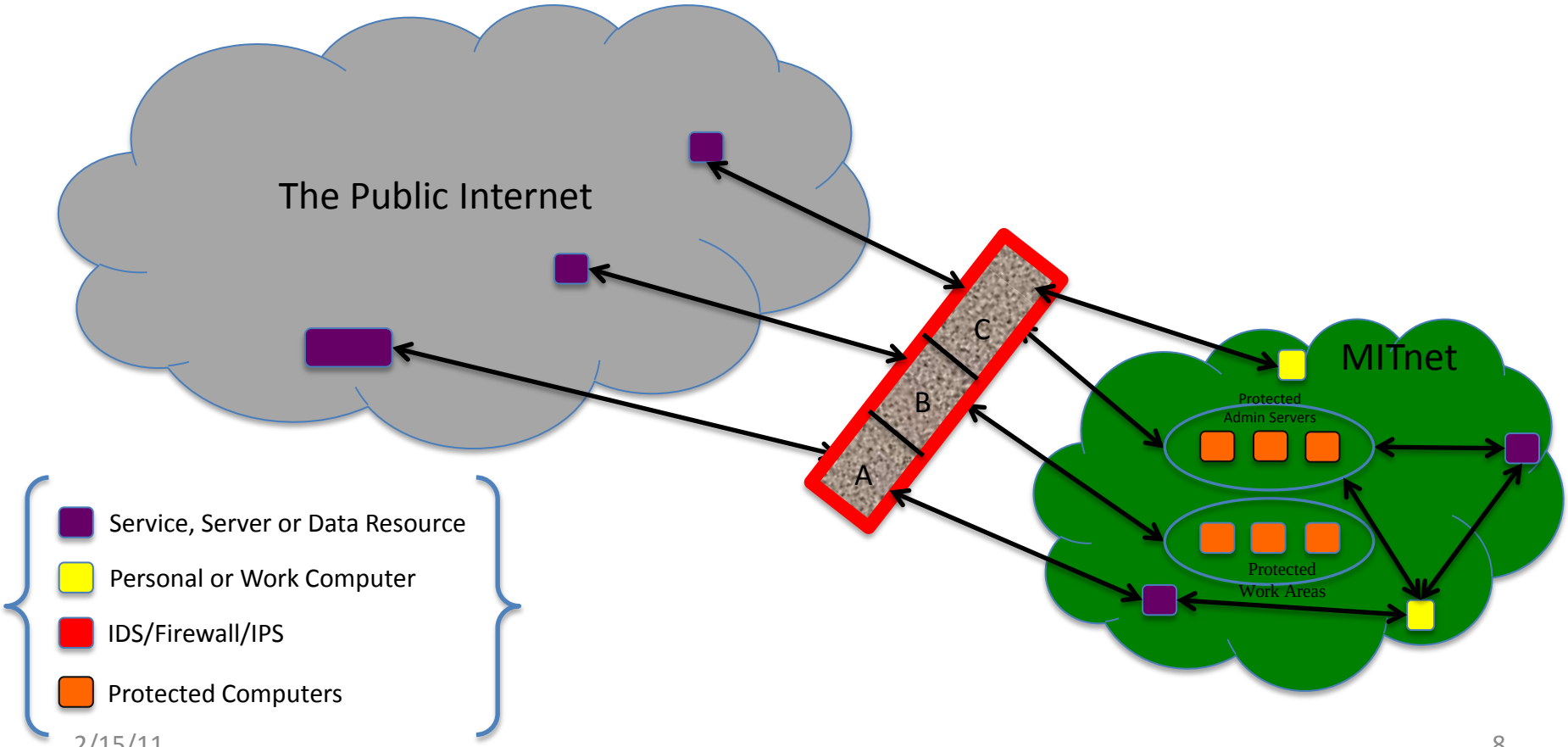
- MIT does not comply with all provisions of MA Data Breach Law/Regulations, particularly in incident detection/response and forensics
- MIT complies with HEOA, but DMCA Notification volumes are soaring, so the measures used may not be enough, and we may need additional technological measures
- Isolating/protecting PCI computers (as well as other devices requiring VERY high protection) remains difficult.

Guiding Principles

- Provide for standards in a decentralized environment
- Academic freedom, privacy and choice
- Technically sound, providing high reliability
- Improve visibility of network needs and issues
- Granularity – no more “one size fits all”
- Protect intellectual property
- Comply with laws and regulations
- Safer computing experience
- Fiscally prudent

Future View

By providing a more managed connection at the border between MITnet and the Public Internet, we increase the visibility of – and our understanding of – the threats and risks that are present, and then how to protect MIT computers and work areas on a very granular level.



What is the plan?

Border Protection

Intrusion Detection
Intrusion Prevention
Border Firewalls
Remediation

The Cisco SCE 8000 Series Service Control Engine delivers high-capacity application and session-based classification and control of application-level IP traffic per subscriber.

The Cisco ASA 5500 Series Adaptive Security Appliances deliver highly effective intrusion prevention capabilities using hardware-accelerated IPS modules.

Network Access

Authenticated Wireless
& Wired Network Access
Logging Policies

Adoption of the 802.1x standard for access to MITnet wireless, with default connections set to be secure, but offering choices for those who need them.

Splunk collects, indexes and harnesses data generated by our applications, servers to troubleshoot problems and investigate security to avoid service degradation or outages. Correlate and analyze complex events spanning multiple systems.

Managed User Experience

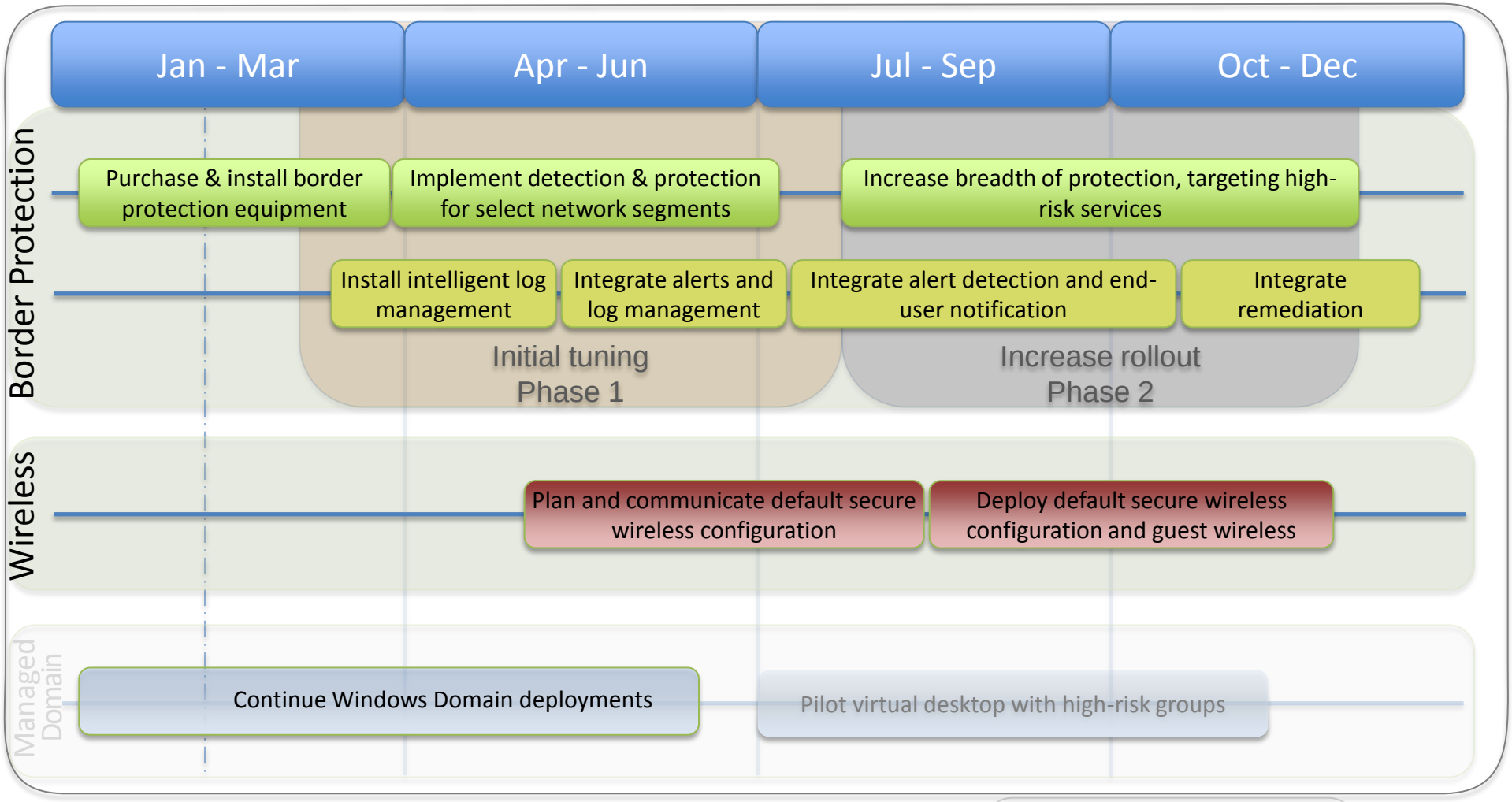
DLC managed domains
IS&T managed domains
Desktop Virtualization

Continue support of an MIT-wide WIN domain for Windows computer; explore Casper for managing Macintosh computers in a similar way.

Move ahead with pilot projects for desktop virtualization in early-adopter, high-risk areas of the Institute.

Network Security Milestone Timeline

Calendar Year 2011



Technology Legend

Cisco ASA 5585 Cisco SCE 8000	Secured wireless
Splunk, RT, Moira	WIN domain Virtual desktop