



Cybersecurity Update

Gary Foster
April 10, 2017

Discussion Topics

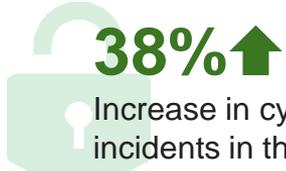
- **Cybersecurity Challenges**
- **Policy Work**
- **Security Awareness & Training**
- **Execution of Policies**
- **Next Steps**



4/10/2017



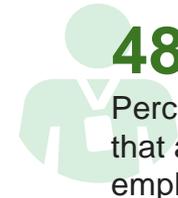
Cybersecurity Challenges



38%↑
Increase in cybersecurity incidents in the past year.¹



5 Months
Average time it takes to detect a security breach.²



48%
Percentage of data breaches that are caused by employees and contractors.²



A complex, moving target

Cyber threats are an increasing risk for MassDOT as professional hackers execute ever more sophisticated attacks against government agencies and private sector companies.



Commonwealth and MassDOT priority

The Commonwealth and MassDOT have identified cybersecurity as top priority. Cybersecurity is critical to MassDOT's ongoing ability to successfully perform its mission.



Cybersecurity begins with us

Cybersecurity is not simply an IT issue, it is an enterprise-wide responsibility. To successfully prevent, identify, and address cybersecurity threats, everyone's involvement is imperative.



4/10/2017

¹ PwC Global State of Information Security Survey

² Ponemon Institute

Policy Work

1	Access Control & Identification and Authentication. User account management, access enforcement and monitoring, separation of duties, and remote access.	 How do we ensure employees have the appropriate accesses to the correct information?
2	Awareness and Training. Timing, frequency, assignment, and documentation of security awareness and role-based security training.	 Are employees aware of their responsibilities to protect confidential information?
3	Audit and Accountability. Audit process controls, including the definition of auditable events, coordination of the audit function and process, and management of audit records.	 Are mechanisms in place to track activities performed on our systems?
4	Security and Risk Assessment. Scope, frequency, and goals of security and risk assessments.	 How do we measure the effectiveness of our information system security assessments?
5	Configuration Management. Configuration management of the configuration systems.	 How can we ensure information is protected when using removable media?
6	Contingency Planning. Maintenance of a contingency plan for information systems.	 How can we ensure our facilities are protected from physical threats such as fires and thefts?
7	Incident Response. Plan and implementation of a response plan.	 How can we evolve with an ever-changing information system security landscape?
8	Maintenance. Scope, frequency, and goals of information system maintenance, security, and risk assessments.	 How do we mitigate risks associated with employee and contractor access to sensitive information systems?
	Media Protection. Managing risks related to media access, media storage, media transport, media protection, and media disposal for both electronic and physical data.	
	Physical and Environmental Protection. Securing the organization's information systems in light of physical and environmental threats.	
	Planning and Program Management. Creating, managing, and maintaining an information security program.	
	Personnel Security. Personnel risks associated with personnel roles and responsibilities in regards to access to sensitive data and systems.	
	Systems and Services Acquisition. Acquisition of systems and services, as well as controls around software development.	
	System and Communication Protection. Protection of MassDOT's network and resources and securing of communications across the network.	
	System and Information Integrity. Maintain system integrity, identify system flaws, and protecting the system from malicious activity.	
	Data Classification. Classification of critical data elements and defines controls for these sensitive data types.	

16

Information security policies created...

189

Internal controls developed...

100%

Policies and internal controls have been signed off as draft by MassDOT senior leadership for implementation

The first policy to be implemented is Security Awareness & Training.



4/10/2017

4



Security Awareness & Training

The Security Awareness & Training program is being delivered in three phases. Phase 1, the current project, defines the program and establishes the approach for subsequent work.

Current Project March – May

- 1 Leadership training and awareness campaign
- 2 Comprehensive training plan
- 3 Multi-channel communications strategy
- 4 Training content requirements

PHASE 1 Define Program

Summer – Fall 2017

PHASE 2 Launch Training

- Deliver online training according to plan
- Track and enforce compliance

PHASE 3 Maintain Program

- Measure outcomes
- Repeat training
- Track and enforce compliance



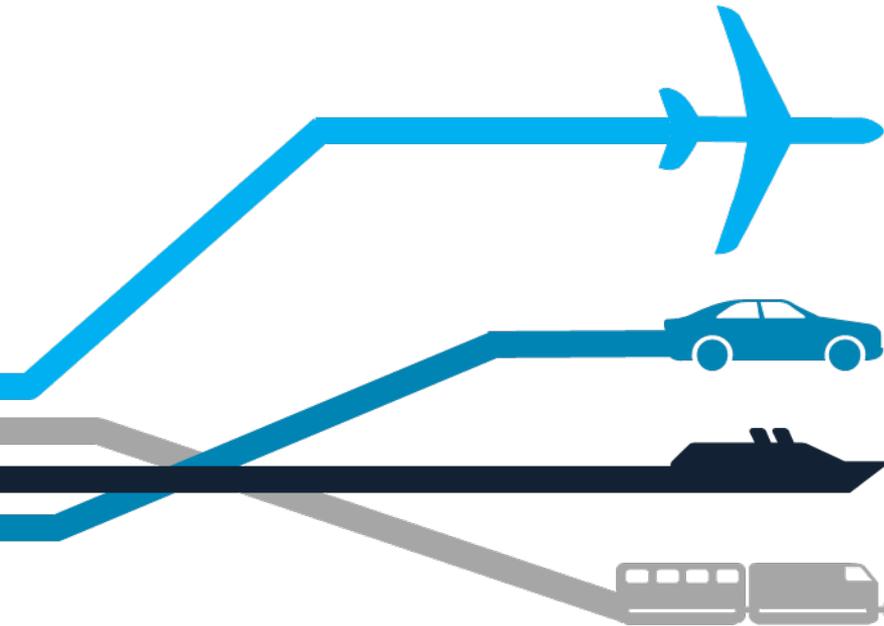
4/10/2017

5



Next Steps

There are several components that are essential to the success of the Security Awareness & Training program.



Leadership support

Will be essential for communicating the value of the program and gaining buy-in

Receptive adoption

Change management is crucial to successfully implementing the training and adopting cybersecurity best practices

Enterprise-wide involvement

Cybersecurity needs to be the responsibility of every division, not only IT

Ongoing input

With your continued input, the implementation will have best chance at succeeding short-term and being sustainable long-term



4/10/2017



7