Photo by Doug Kerr
Used With Permission

Cyber Security Update

October 16, 2017

massDOT
Massachusetts Department of Transportation

Agenda

- Summary – Key messages
- Information security a top priority
- Embarked on a journey to mature our security posture
- Our organization is aware and prepared for this journey
- Step 1: Policies covering required controls developed and approved
- Step 2: We've defined a robust strategy and multi-year plan
- We are investing in people: Security Awareness Training
- Incident Response Planning has started and more work required
- Next steps

Overview

1 Today's threat landscape is evolving and it is extremely complex. It's not a matter of "if", it is a matter of "when".

2 Information security became a priority in 2016 and it's a top concern of the governor. We're working across our organization and with EOTSS to secure resources and expect increasing long term capital investment in this area.

3 Based on recent assessments, we need to work on improving our security posture and approach information security as an enterprise-wide risk management issue.

4 As a foundational step, we are rolling out a enterprise-wide security awareness training program and empowering our people to safeguard the organization's digital assets.

Information security has become a top priority for us

38% ↑

Increase in information security incidents in the past year.[1]

5 Months

Average time it takes to detect a security breach.[2]

48%

Percentage of data breaches caused by employees and contractors.[2]

A complex, moving target

Cyber threats are an increasing risk for MassDOT/MBTA as professional hackers execute ever more sophisticated attacks against government agencies.

Commonwealth and MassDOT priority

The Commonwealth and MassDOT/MBTA identified cyber security as critical priority, and it is a top concern of Governor Baker. Information and cyber security are critical to the agency's ability to perform its mission.

Impact of a security incident can be significant

In transportation, a security incident can cause serious damage. It can impact the safety of our citizens, disrupt operations, destroy our reputation, or damage financials.

[1] PwC Global State of Information Security Survey

[2] Ponemon Institute

Mature cybersecurity posture in alignment with Commonwealth (EOTSS)

Substantial accomplishments have been made since last October:

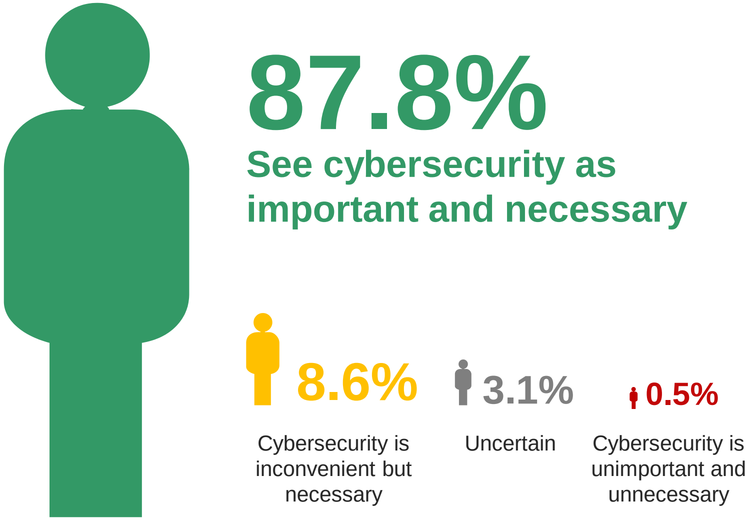
- 16 Standard Enterprise Policies Defined
- Robust Strategy and Roadmap
- Security Awareness Campaign
- 3rd Party Testing and remedies
- Beginning of Incident Response Planning *(work in progress)*
- Security Awareness Training *(active)*

Substantial work remains to allow us to adequately manage our risks throughout the organization:

- Implementation of Policies
  - ❖Multi-year roadmap
  - ❖People, process, technology
- Adoption of a Security Awareness Culture
  - ❖Individual responsibilities
  - ❖Understanding cybersecurity is not an IT issue but an organizational responsibility

Our organization is ready for this journey

Based on a survey distributed to all MassDOT/MBTA information system users, our employees see information security as important, and are receptive to training and additional knowledge.



87.8%

See cybersecurity as important and necessary

8.6%

Cybersecurity is inconvenient but necessary

3.1%

Uncertain

0.5%

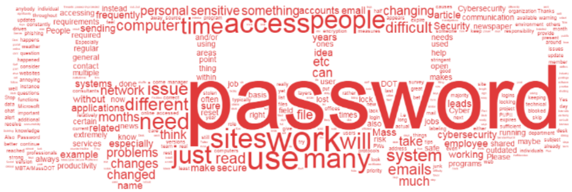
Cybersecurity is unimportant and unnecessary

Of the comments provided, 41% related to the need to change current practices; *passwords* were the most frequently cited pain point.

41%

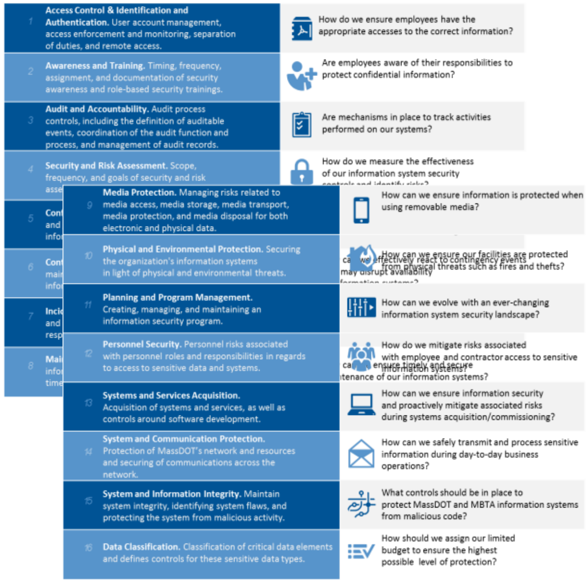
need
information
training
work
phishing
important
password
computer
can
use
users
secure
Security
personal
computers
access
system
Cyber
MassDOT
passwords
time
one
job
make
many
etc
needs
critical
able
know
practices
disaster
event
new
staff
number
attack
changing
importance

39%



*Surface area of graphics are scaled to match percentage proportions

Step 1: Policies covering all required controls developed and approved



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 trainings.	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 asse	How do we measure the effectiveness of our information system security controls and identify risks?
5	Con and info	
6	Con mai info	ca we effectively react to contingency events may disrupt availability formation systems?
7	Incic and resp	
8	Mai info time	ca ensure timely and secure tenance of our information systems?

9	**Media Protection.** Managing risks related to media access, media storage, media transport, media protection, and media disposal for both electronic and physical data.	How can we ensure information is protected when using removable media?
10	**Physical and Environmental Protection.** Securing the organization's information systems in light of physical and environmental threats.	How can we ensure our facilities are protected from physical threats such as fires and thefts?
11	**Planning and Program Management.** Creating, managing, and maintaining an information security program.	How can we evolve with an ever-changing information system security landscape?
12	**Personnel Security.** Personnel risks associated with personnel roles and responsibilities in regards to access to sensitive data and systems.	How do we mitigate risks associated with employee and contractor access to sensitive information systems?
13	**Systems and Services Acquisition.** Acquisition of systems and services, as well as controls around software development.	How can we ensure information security and proactively mitigate associated risks during systems acquisition/commissioning?
14	**System and Communication Protection.** Protection of MassDOT's network and resources and securing of communications across the network.	How can we safely transmit and process sensitive information during day-to-day business operations?
15	**System and Information Integrity.** Maintain system integrity, identifying system flaws, and protecting the system from malicious activity.	What controls should be in place to protect MassDOT and MBTA information systems from malicious code?
16	**Data Classification.** Classification of critical data elements and defines controls for these sensitive data types.	How should we assign our limited budget to ensure the highest possible level of protection?

16	**Information security policies created…**
189	**…which consist of a number of internal controls**
100%	**All policies and internal controls have been signed off by Secretary Pollack and MassDOT/MBTA leadership.**

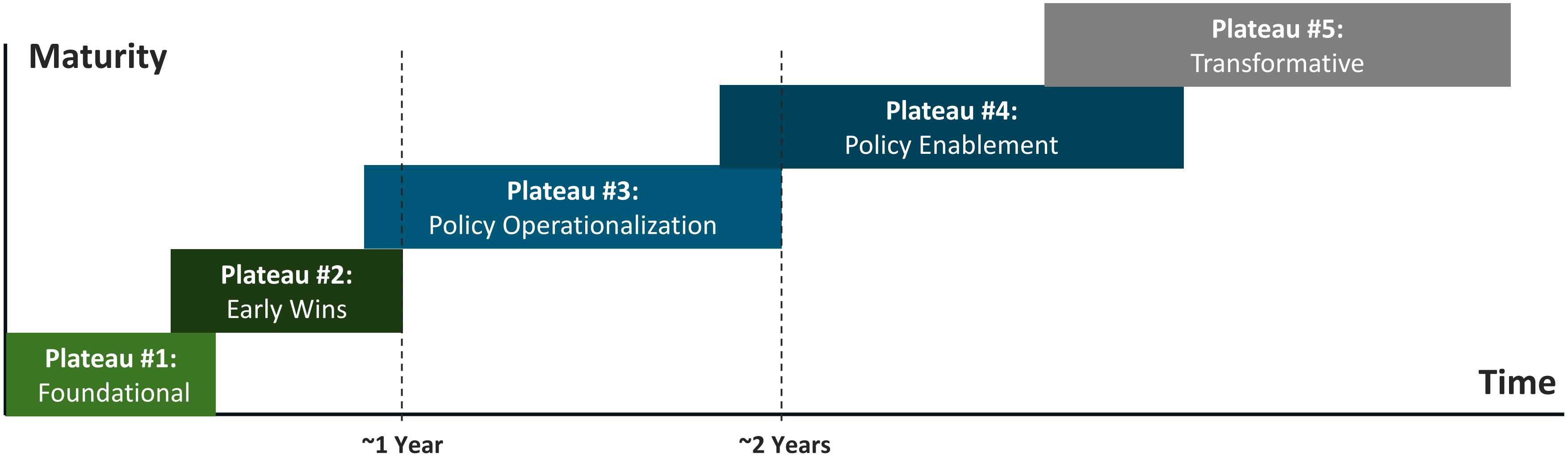
Policy Execution

Policy #2 – Awareness & Training

Policy #7 – Incident Response and Training

Step 2: We've defined a robust strategy and a 3-5 year execution plan

Projects have been grouped into 5 plateaus to provide increasing maturity over a period of time. This step-wise approach enables capturing benefits incrementally, limiting implementation risks and reducing complexity.



Investing in people: Annual Mandatory Security Awareness Training

Pilot Training – *August 25 – September 25, 2017*

213
MassDOT/MBTA staff were invited to take the training

70%
Of staff invited completed the training

84% ☺
Agreed or strongly agreed they found the course worthwhile

→

Enterprise-wide training *to launch October and last until December 2017*

7000+
All MassDOT/MBTA information system users

3 Tiers
1. General
2. Sensitive Information
3. Merchant (PCI)

Awareness & Communications – *Ongoing*

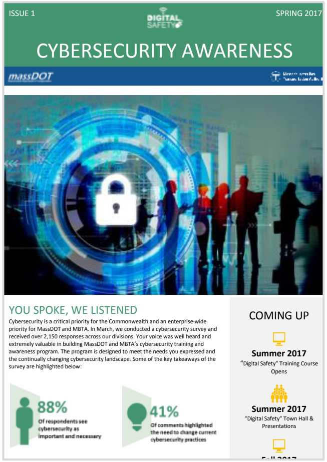
PASSWORD

M1x 1t Up

M@k3 1t $tr0ng

DIGITAL SAFETY
massDOT

Posters



ISSUE 1 | DIGITAL SAFETY | SPRING 2017

CYBERSECURITY AWARENESS

massDOT

YOU SPOKE, WE LISTENED

Cybersecurity is a critical priority for the Commonwealth and an enterprise-wide priority for MassDOT and MBTA. In March, we conducted a cybersecurity survey and received over 2,150 responses across our divisions. Your voice was well heard and extremely valuable in building MassDOT and MBTA's cybersecurity training and awareness program. The program is designed to meet the needs you expressed and the continually changing cybersecurity landscape. Some of the key takeaways of the survey are highlighted below:

88% Of respondents see cybersecurity as important and necessary

41% Of comments highlighted the need to change current cybersecurity practices

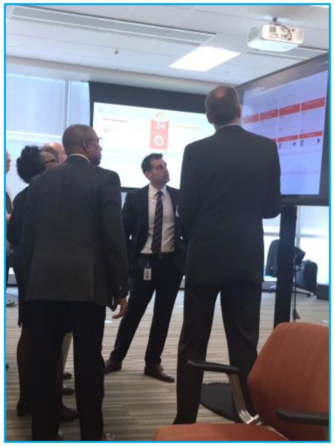
COMING UP

Summer 2017
"Digital Safety" Training Course Opens

Summer 2017
"Digital Safety" Town Hall & Presentations

Fall 2017

Newsletters



Game of Threats and Roadshows

National Cyber Security Awareness Month

Phishing Campaign

massDOT Massachusetts Department of Transportation

Incident Response Planning has started, but more work is needed

As a starting point, we recently developed a draft Executive-level Information Security Incident Response Plan. However, foundational elements such as IR SOPs must also be developed to enable our organization to effectively respond to incidents.

✓ Incident Response Rapid Assessment

Three key recommendations that we are working on: creating effective channels of communication, establishing accountability, and aligning IT Security skills/resources with capabilities needed.

□ Draft Executive-level Plan

Provides guiding principles for identifying, triaging, Containing, and responding to information security incidents.

□ Practice

Two simulations and one table top exercise completed. More practice needed and will be planned.

❖ Next steps

Additional planning/work needed for departmental SOPs, Disaster Recovery planning and Business Continuity planning

Next Steps

- **Roll out first annual security awareness training**
- **Support ongoing Payment Card Industry (merchant) audits**
- **Complete technical remediation work including the following areas:**

  Removing shared passwords for privileged accounts, reducing administrator accounts, increasing password complexity, increase automated monitoring of security critical infrastructure, network segmentation assessment

- **Build momentum on policy and internal control implementation**