



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

January 9, 2013



ISOAG January 2013 Agenda

- | | | |
|------|----------------------------------|---|
| I. | Welcome & Opening Remarks | Michael Watson, VITA |
| II. | Mobile Device Risk Assessments | David Frei, Capital One |
| III. | IREC End User Survey | Ed Miller, VITA |
| V. | Exceptions | Michael Watson, VITA |
| VI. | Upcoming Events & Other Business | Michael Watson, VITA |
| VII. | Partnership Update | Bob Baskette, VITA
Michael Clark, NG |

Conducting a Risk Assessment for Mobile Devices

David Frei

Capital One

Director, Digital/Information Security Specialist

This Presentation
Has Been Intentionally
Omitted



Virginia Information Technologies Agency

IREC End-User Security Awareness Survey

Ed Miller
Security Analyst, VITA



IREC End-User IT Security Survey

- On Nov 5, we sent out web links for a survey to 1000 randomly selected COV employees. All employees work at agencies that are in the IT partnership.
- We received 321 responses and participants were anonymous.
- There was also some general demographic information collected, i.e. employee role, level in the agency, etc.



Purpose of the Survey

IREC launched its inaugural **End-User Awareness Survey** in 2007 to measure end-user behavior & to identify how information security functions can best drive users toward increasing the security of their behavior.



Purpose of the Survey

1. Evaluation of users' behavior, psychology, and perception of security awareness campaigns at their agency.
2. Comparison of how the COV's behavior and awareness activities fare against those of the private sector and other government entities.
3. Recommendations on the top areas of focus in order for the COV to improve overall behavior and tactics we can use for particular areas of concern.



IREC End-User IT Security Survey

Users from the Commonwealth were benchmarked against users from the other participating organizations.

Benchmarking Dataset and Participation Details

All Participating Organizations:	39,535
Government Agency & Other:	4,627
Commonwealth of Virginia:	321

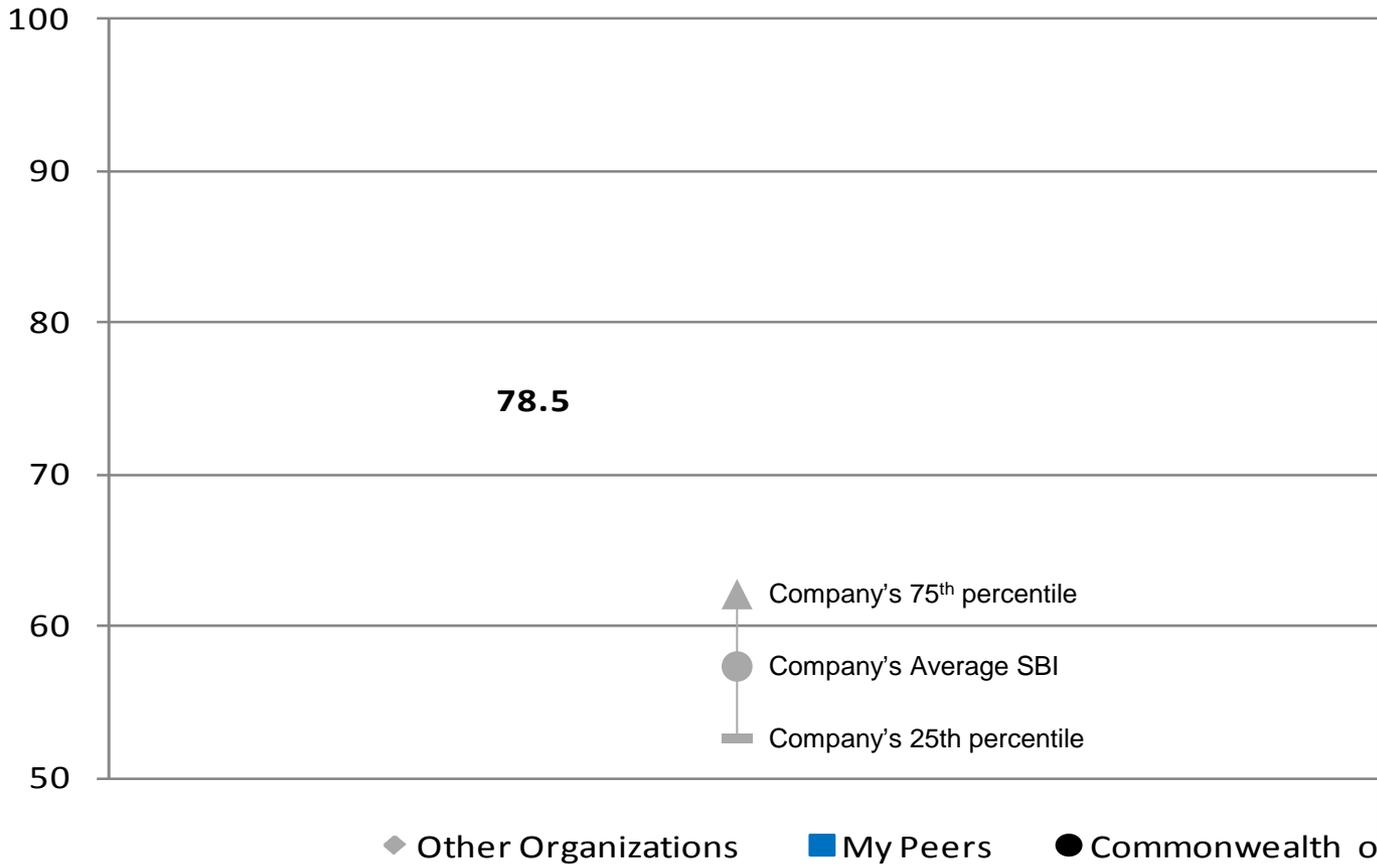


Example survey questions

- Do you ever write down one or more of your work-related password(s) so that you don't forget them?
 - 1. Frequently
 - 2. Often
 - 3. Sometimes
 - 4. Seldom
 - 5. Never
- How often do you copy or email files containing sensitive information so that you can work on them at home or on the road?
 - 1. Frequently
 - 2. Often
 - 3. Sometimes
 - 4. Seldom
 - 5. Never



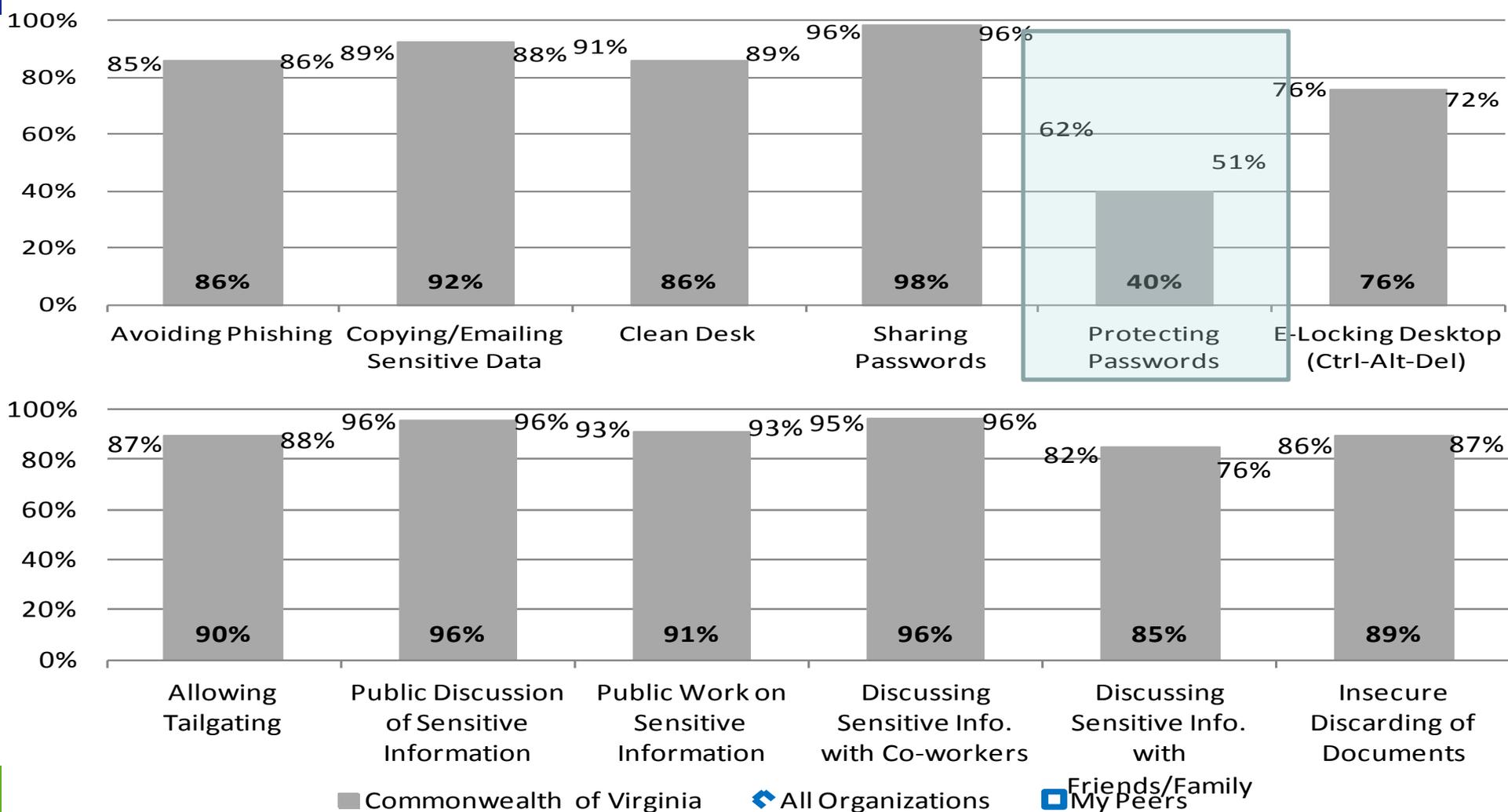
END-USER BEHAVIOR SECURITY @ COV



The index is measured on a 100-point scale where 0 points indicate only insecure behavior, and 100 points indicate perfect behavior.

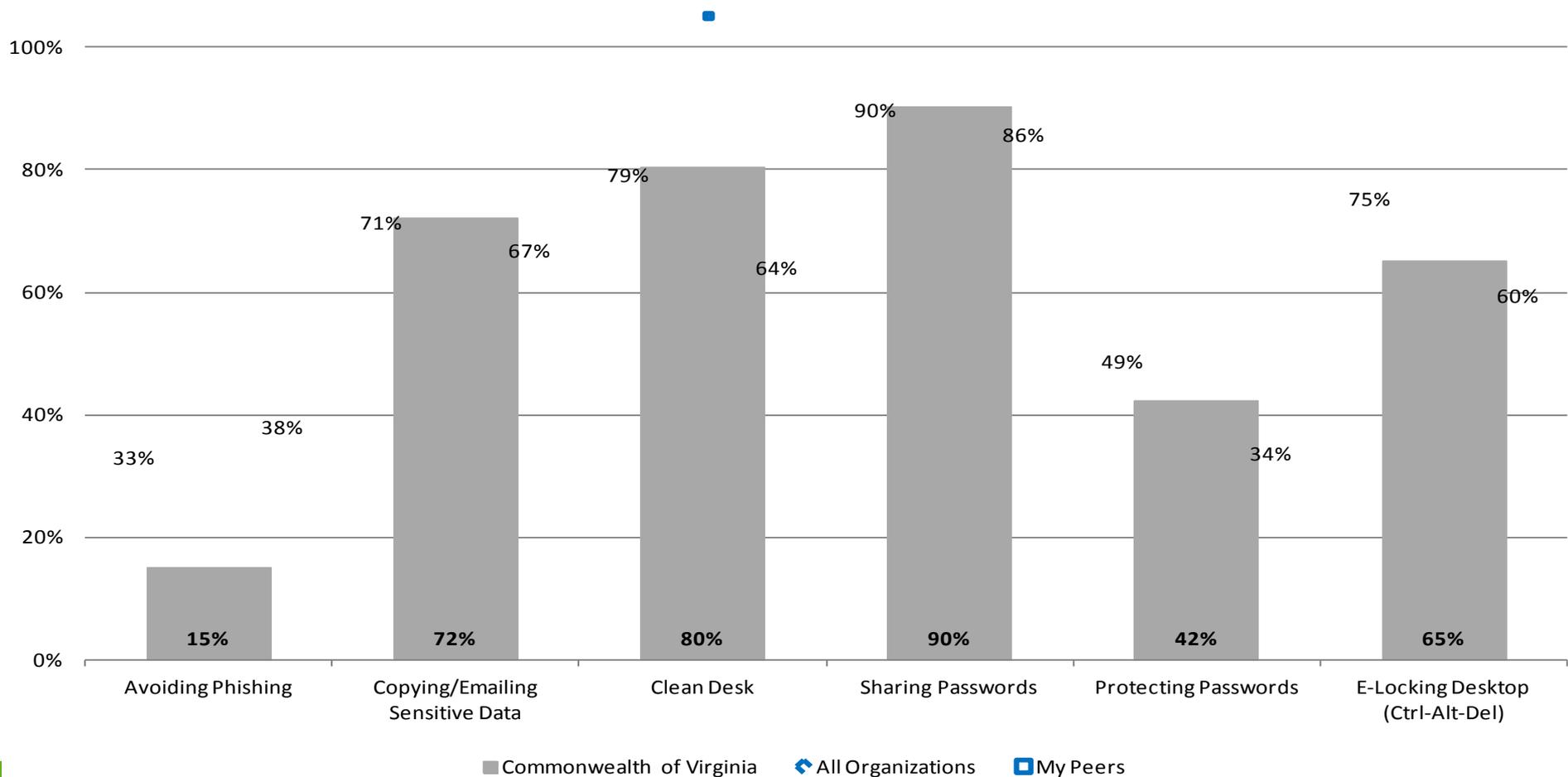


END-USER SECURITY ON KEY BEHAVIORS



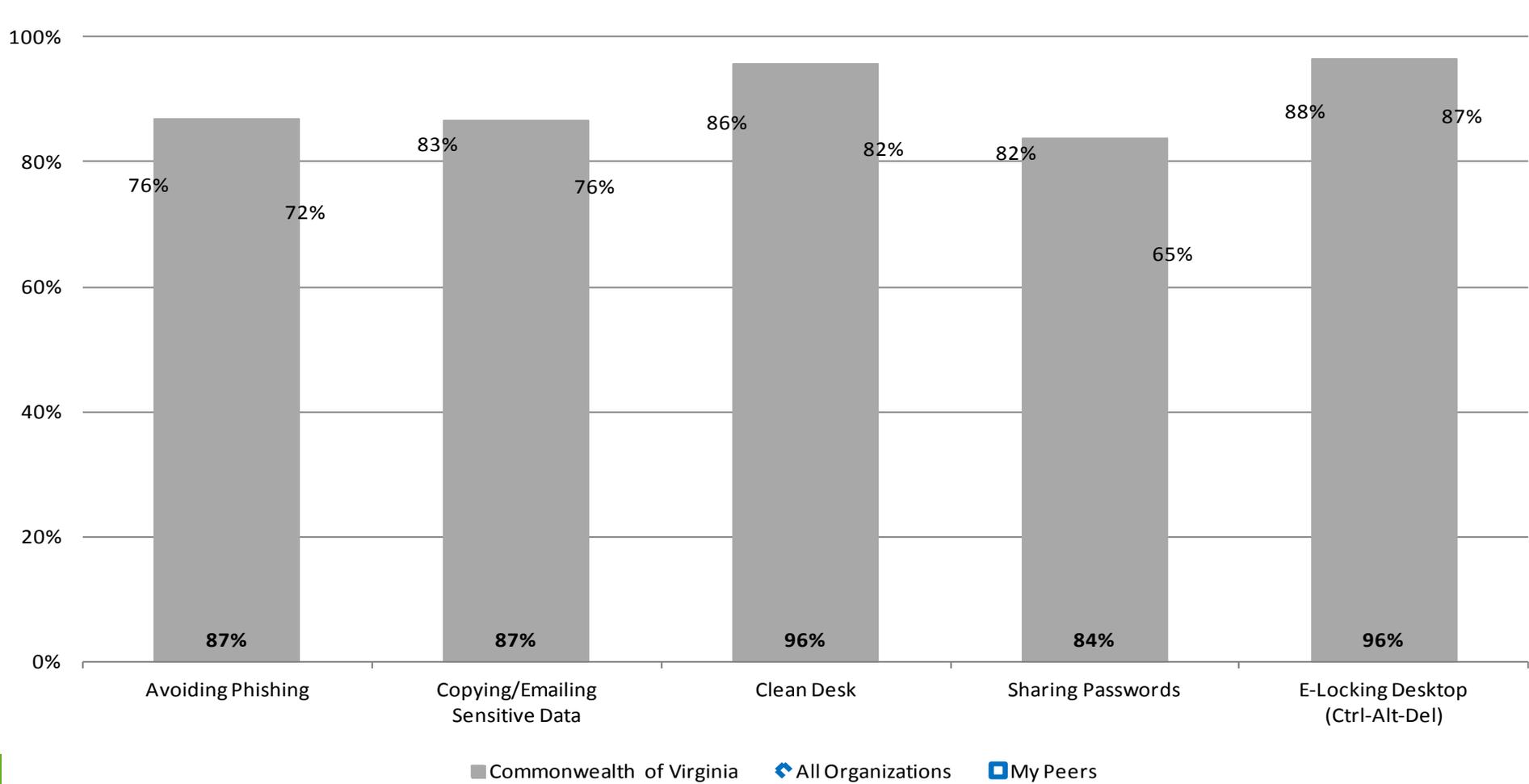


POLICY KNOWLEDGE OF KEY BEHAVIORS

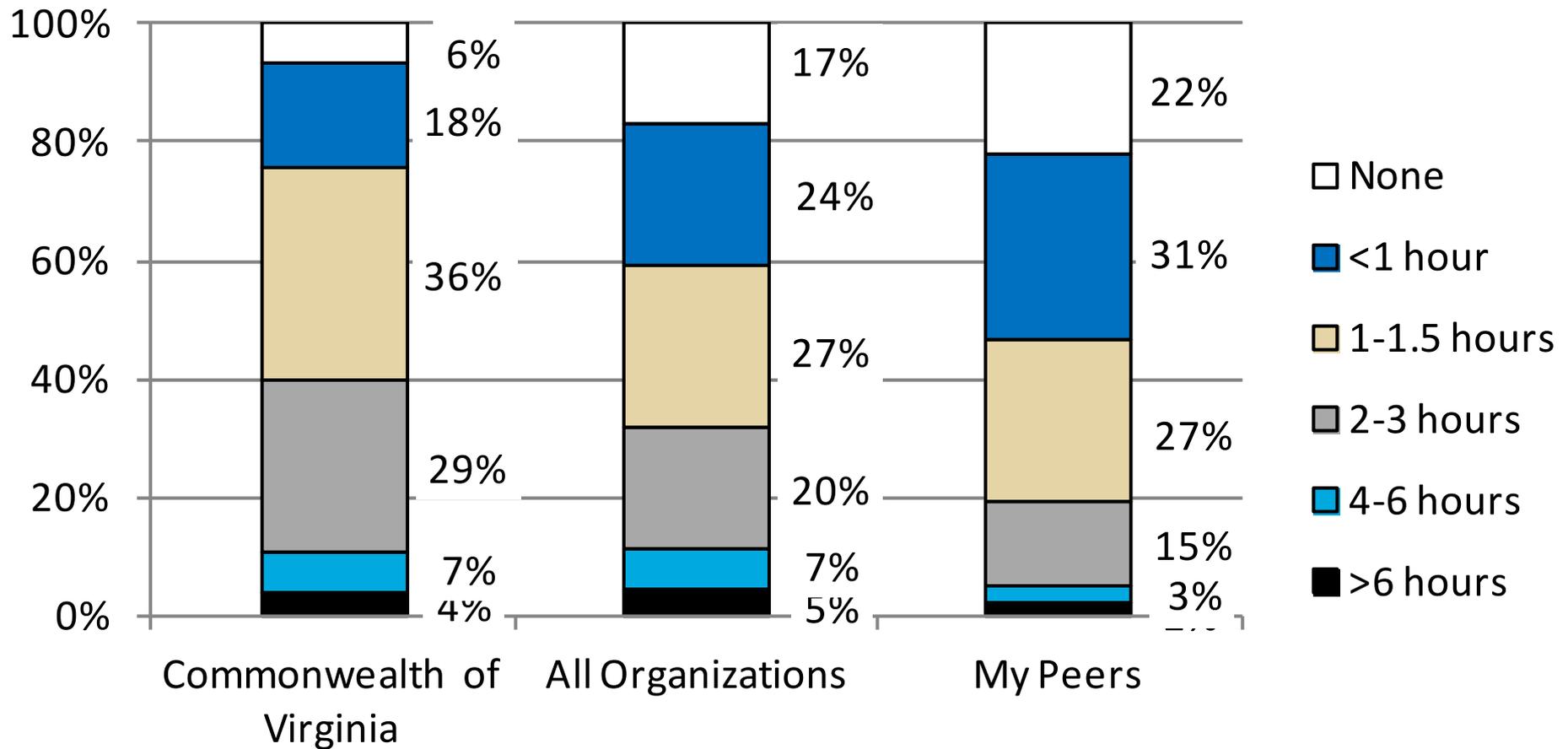




RISK PERCEPTION OF KEY BEHAVIORS

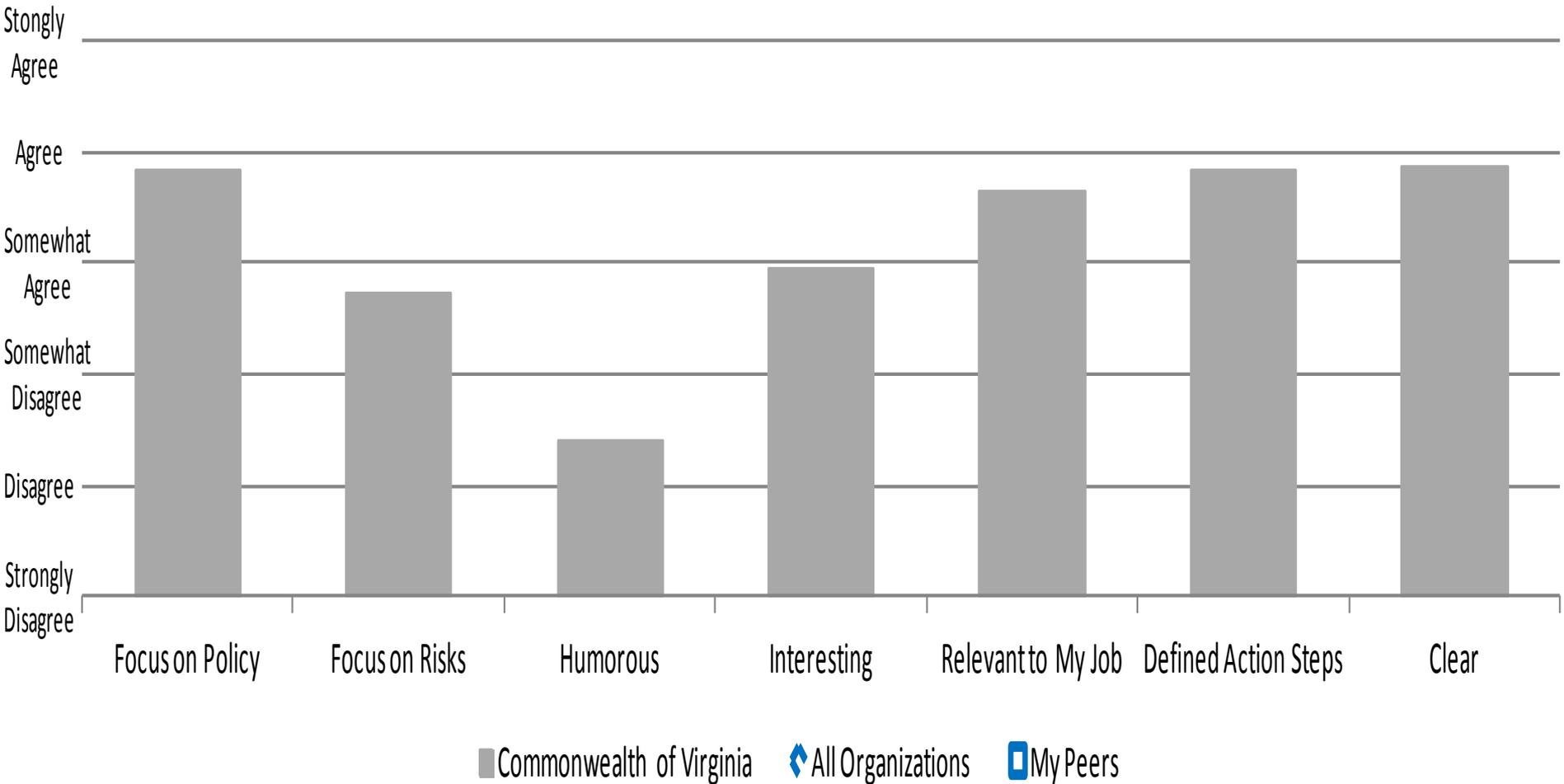


Quantity of IT Security Training Received



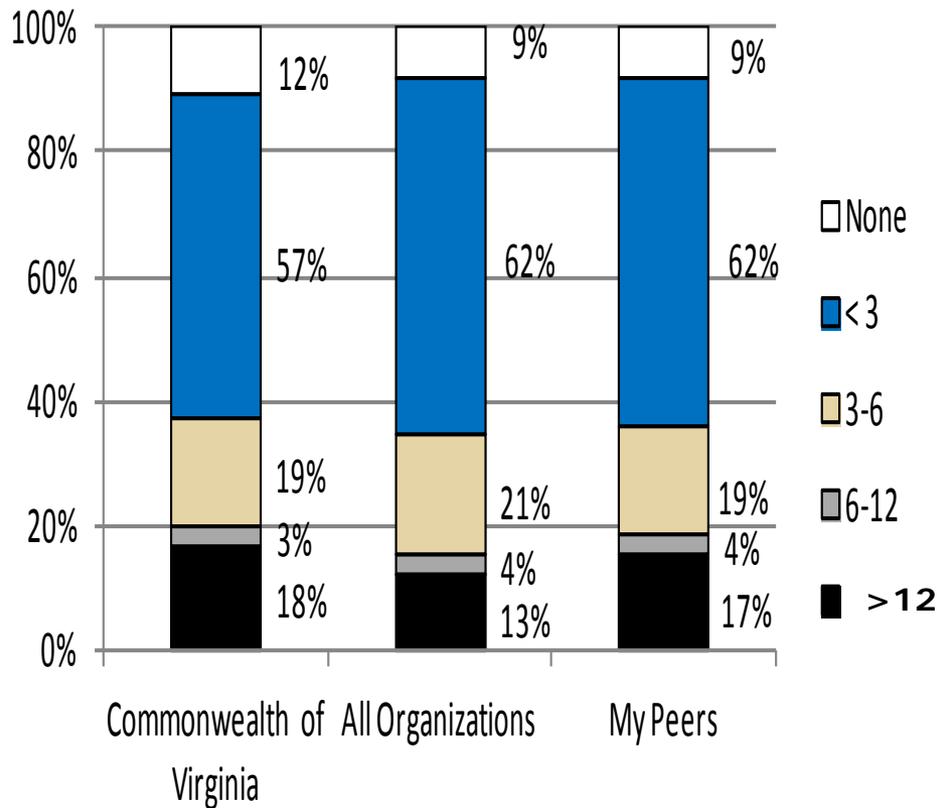


Quality of IT Security Training Received

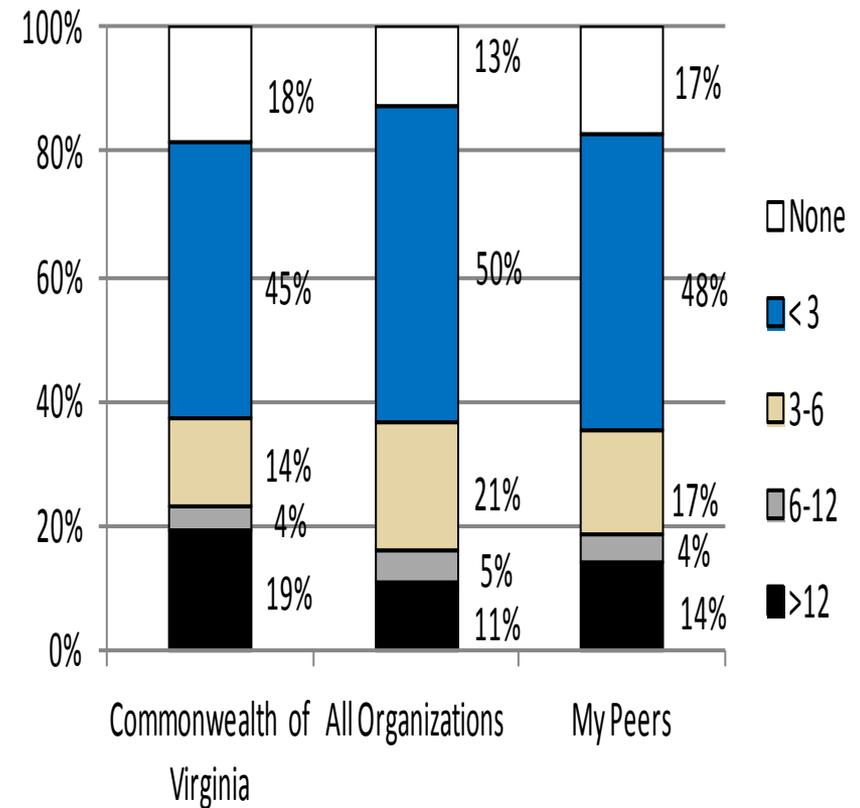


Quantity of Communications Rec'd

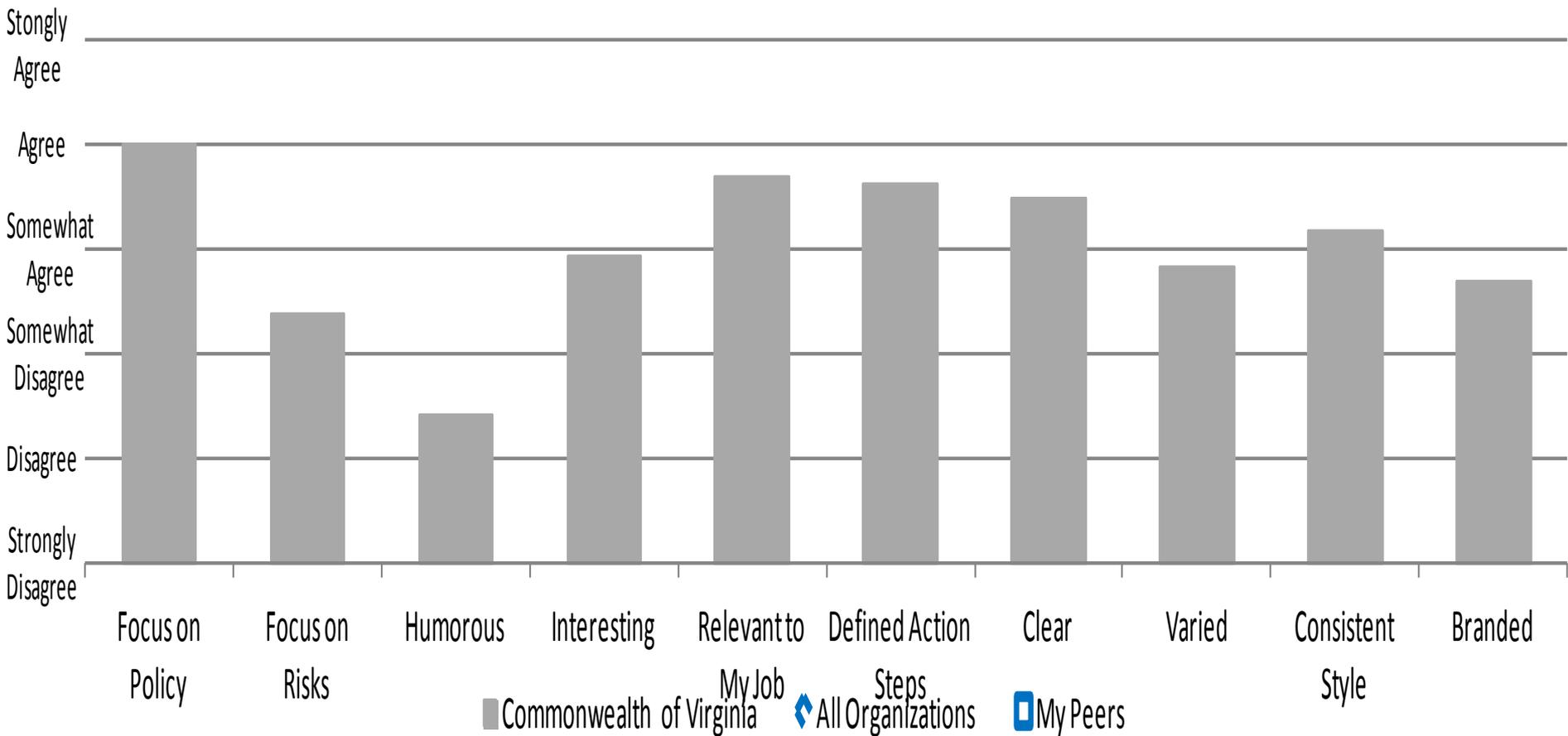
Direct Communications



Indirect Communications



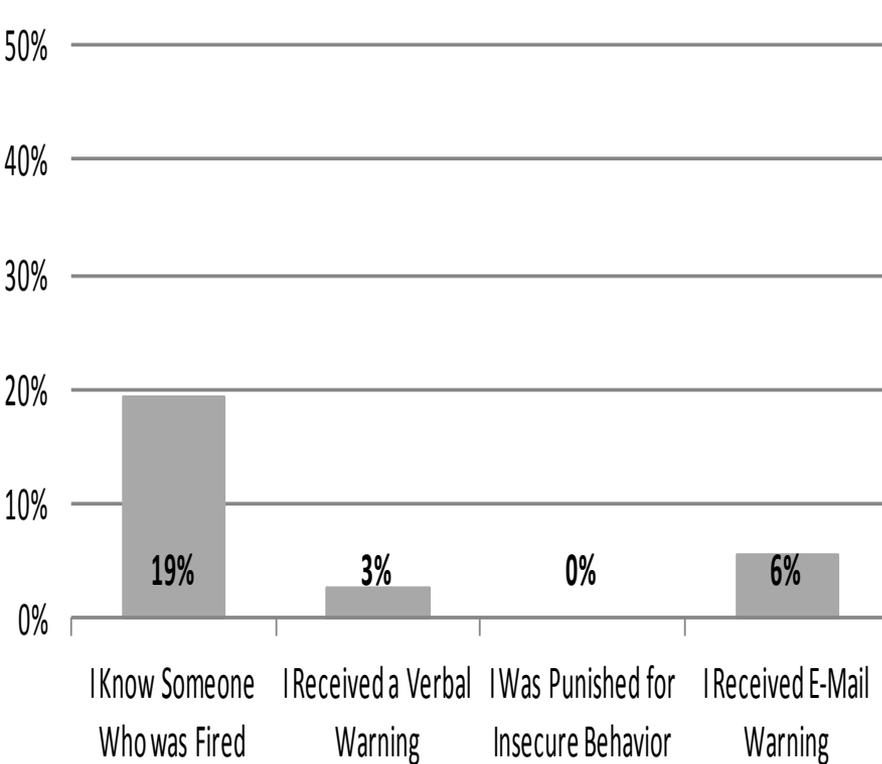
Quality of Communications Rec'd



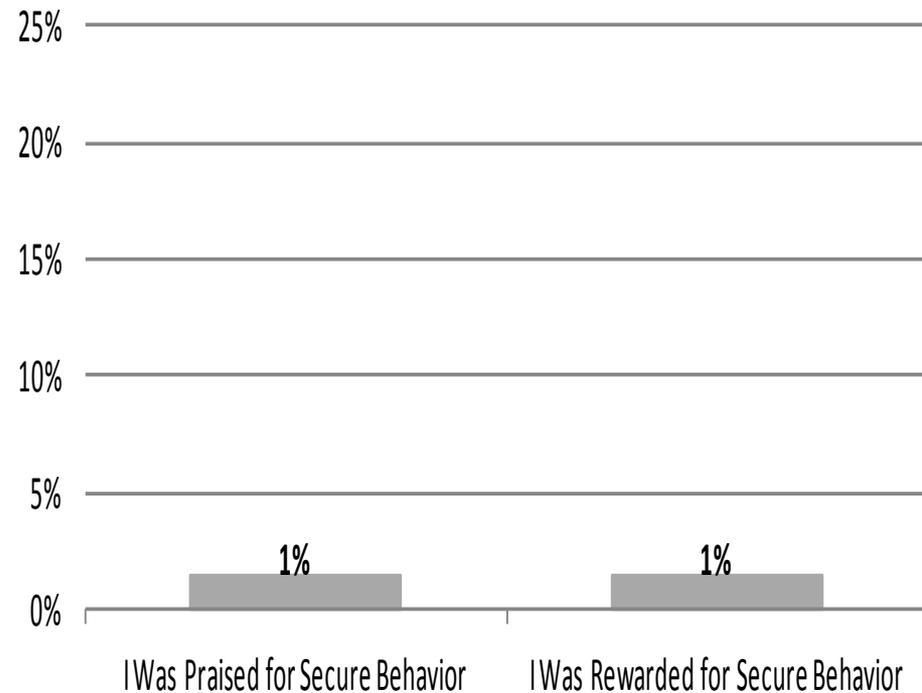


Penalties and Rewards

User Experience of PENALTIES



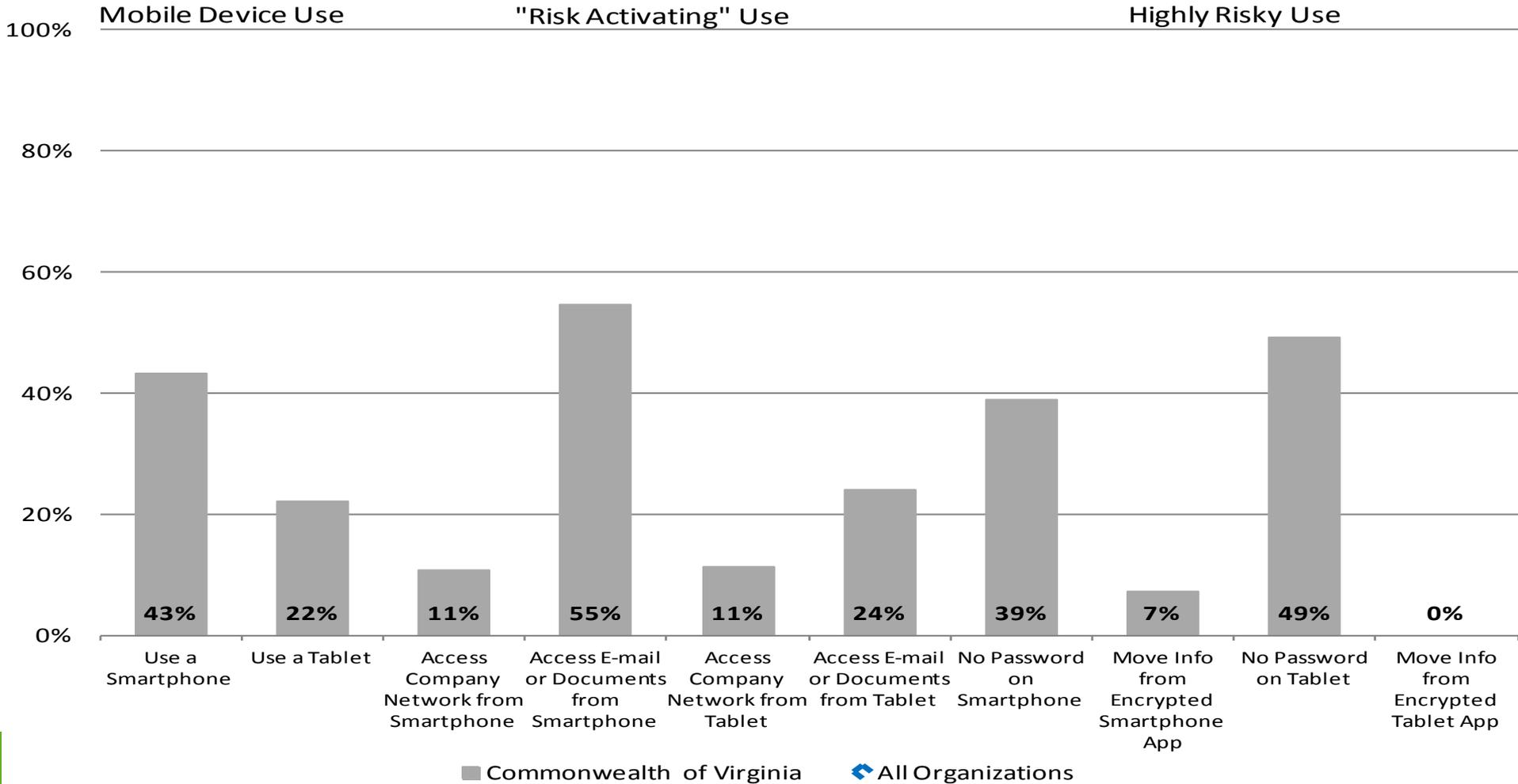
User Experience of REWARDS





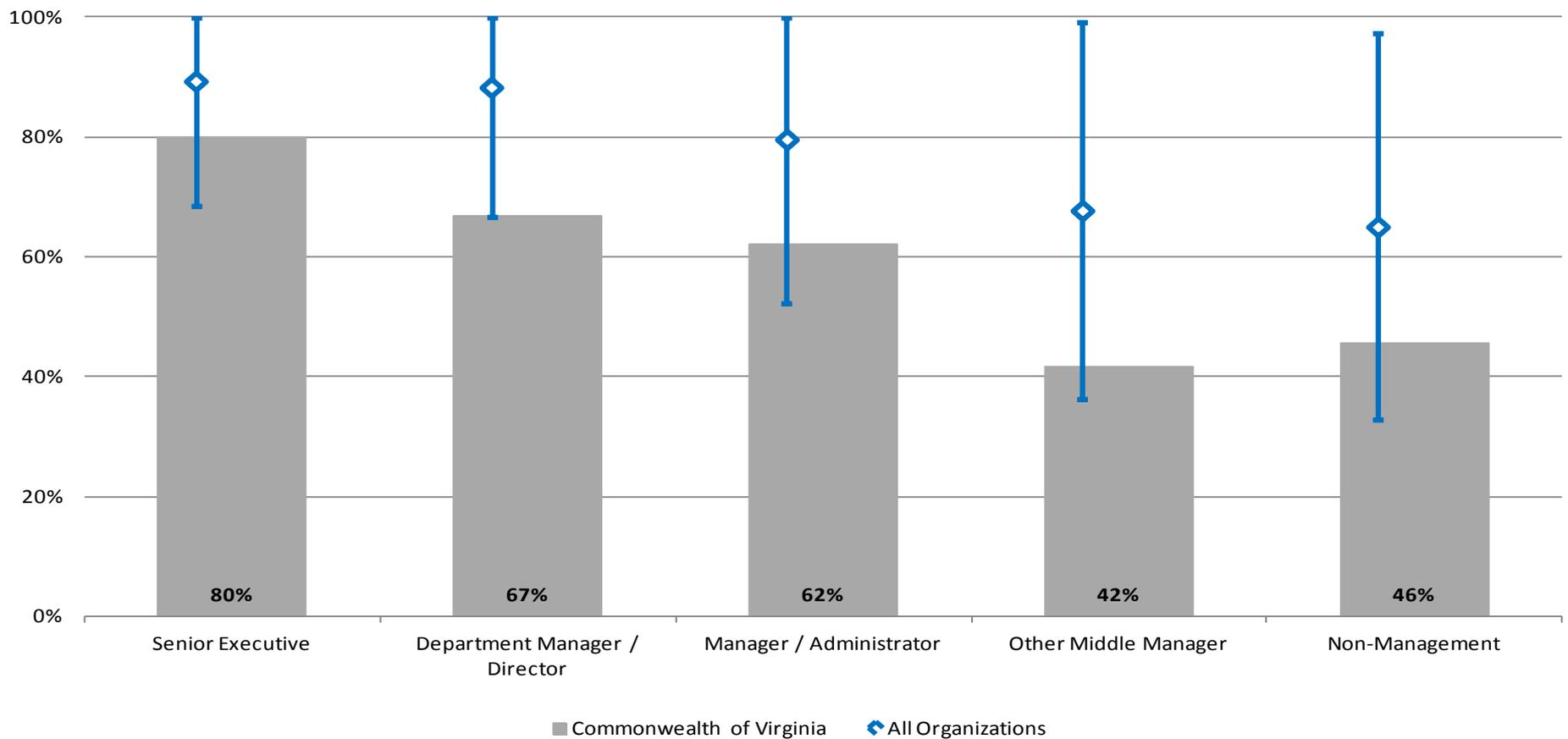
Includes both COV issued devices & personally owned devices.

Frequency of Mobile Device Use





Mobile Device Use by Level





Opportunities for Improvement

Rank	Activity Type	End User Awareness Activity
1	Communication	Present communication clearly & logically
2	Training	Focus training on policies & procedures
3	Training	Present training clearly & logically
4	Penalty	Ensure that employees do not tolerate insecure behavior
5	Training	Ensure training is relevant to user's day-to-day work
6	Communication	Ensure that communication contains defined actions to improve security
7	Communication	Focus communication on policies & procedures
8	Training	Ensure that training contains defined actions to improve security
9	Communication	Ensure communication is relevant to user's day-to-day work
10	Penalty	Provide special training for security violations



Opportunities for Improvement

Rank	Activity Type	End User Awareness Activity
11	Penalty	Send emails from SECURITY after policy violations
12	Training	Ensure that training is interesting
13	Penalty	Revoke some IT privileges for behavior violations
14	Training	Focus training on the financial costs to the agency from insecure behavior
15	Penalty	Give negative marks on performance review for insecure behavior
16	Communication	Ensure that communication has a consistent "look & feel"
17	Training	Increase the number of hours of training
18	Communication	Ensure that communication is interesting
19	Reward	Encourage employees to provide feedback on security
20	Penalty	Give official reprimands for violations



Opportunities for Improvement

Rank	Activity Type	End User Awareness Activity
21	Communication	Increase the number of indirect communications
22	Communication	Focus communications on the financial costs to the agency of IT security violations
23	Penalty	Fire information security violators
24	Penalty	Consider information security in performance reviews
25	Penalty	Have violations lead to demotions or role changes
26	Communication	Ensure communication contains an identifying logo, mascot or slogan
27	Reward	Visibly reward people for secure behavior
28	Communication	Increase the number of direct communications
29	Reward	Give positive marks on performance reviews for secure behavior
30	Reward	Give praise from manager or coworkers for secure behavior



Opportunities for Improvement

Rank	Activity Type	End User Awareness Activity
31	Penalty	Give public criticism for insecure behavior
32	Communication	Ensure that communication is not repetitive
33	Reward	Have managers give private praise for secure behavior
34	Training	Ensure that training is humorous
35	Penalty	Have managers give informal warnings for insecure behavior
36	Reward	Send emails from SECURITY for thanks for secure behavior
37	Reward	Give public praise or rewards for secure behavior
38	Reward	Give cash or other material reward for secure behavior
39	Communication	Ensure that communication is humorous



Questions

- If you would like a copy of the complete report let me know.
- Ed Miller
- 804-416-6027
- Edward.miller@vita.virginia.gov
- Thank you!



Exceptions to Security Requirements

Michael Watson
Chief Information Security Officer



1.5 Exceptions to Security Requirements

If an Agency Head determines that compliance with the provisions of this *Standard* or any related information security standards would adversely impact a business process of the agency, the **Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO.**



1.5 Exceptions to Security Requirements

For each exception, the requesting agency shall fully document:

1. Business need
2. Scope and extent
3. Mitigating safeguards
4. Residual risks
5. Specific duration
6. Agency Head approval



1.5 Exceptions to Security Requirements

Each request shall be in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks.

Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks.

Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken.



1.5 Exceptions to Security Requirements

An exception will not be accepted for processing unless all residual risks have been documented and the Agency Head has approved, indicating acceptance of these risks.

The exception request must be submitted by the Agency Head or Agency ISO. Denied exception requests may be appealed to the CIO of the Commonwealth.



Exception Request Form

- APPENDIX A – INFORMATION SECURITY POLICY AND STANDARD EXCEPTION REQUEST FORM
- The **EXCEPTION REQUEST FORM** must be submitted by an agency to request an exception to **any requirement** of this *Standard and the related Information Security Policy...*

COV Information Security Policy & Standard Exception Request Form

Agency Name: _____ **Contact for Additional Information:** _____

Policy/Standard requirement to which an exception is requested: _____

Note: This request is for an exception(s) to a component of the Commonwealth policy and/or standard(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:**
2. Describe the scope including quantification and requested duration (not to exceed one (1) year):
3. Describe all associated risks:
4. Identify the controls to mitigate the risks:
5. Identify all **residual** risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

Printed name Agency Head

Signature

Date



Control Implementation

- We have noted in many Corrective Action Plans and Risks Assessments that have been submitted, that many required SEC501 security controls take months, if not years, to implement.
- The security of your agency and of the Commonwealth requires that gaps in essential controls are implemented or mitigated as quickly as possible.



Filing an Exception Request

- For all audit findings, related to a required SEC501 security control
AND
For all SEC501 control gaps reported in an agency Risk Assessment for a sensitive system:
- An agency must file an Exception Request with VITA if the agency will need **longer than 90 days** to implement the control or acceptable mitigation.



Questions





Virginia Information Technologies Agency

Upcoming Events





2013 General Assembly

***2013
General Assembly Session
Begins
January 9, 2013***



CIS/MS-ISAC & SANS

Center for Internet Security & SANS Institute for Security Awareness Training

As part of the Center for Internet Security and SANS partnership agreement they are offering this aggregate purchasing opportunity for state, local, territory and tribal governments, as well as related educational and not-for-profit entities,

during the ***December 1, 2012 to January 31, 2013*** timeframe.

**As a quick reminder, while looking over the MS-ISAC offering, bear in mind that this is a good opportunity, but your agency needs to follow the Virginia Public Procurement Act (VPPA) and their agencies' procurement rules.

For more information:

<http://alliance.cisecurity.org/opportunity/sans-securing-the-human-purchasing-opportunity.cfm>



DSIA Training

Auditing Cloud Services

Instructor: David Cole (SysAudits)

Date: January 29 & 30, 2013

Time: 8:15-4:45

Location: James Monroe Building
DOE Conf. Rm., 22nd FL

Cost: \$ 320.00

Register: <https://hrtraining.doa.virginia.gov>



Future ISOAG Dates

Feb 6 1:00 – 4:00 pm @ CESC

Keynote Speaker: Dr. Ron Ross, NIST

Mar 6 1:00 – 4:00 pm @ CESC

Keynote Speaker: Lyn Rahilly, Privacy Officer

U.S. Customs and Immigration Enforcement

Apr 3 1:00 – 4:00 pm @ CESC

Keynote Speaker: Lori Broache,

Continuity Management Solutions

ISOAG meets the 1st Wednesday of each month in 2013



Submit Events

- If your group or organization is promoting a security related event and would like to have it communicated to the Information Security Officer community:

Please submit all upcoming events to:

CommonwealthSecurity@VITA.Virginia.Gov



ISOAG-Partnership Update

*IT Infrastructure Partnership Team
Bob Baskette*

Jan 9, 2013



NORTHROP GRUMMAN



ADJOURN

