!mpactmakers

Better Business. Better Community.

Building Engagement through Role-based Information Security Training

Scott Hammer, PMP, CISM, CRISC

April 12, 2019

01 | The importance of role-based information security training

Why worry about engagement?

In providing role-based information security training, we're often asking people to process a lot of change; engagement eases the process and increases effectiveness.

Link: https://www.youtube.com/watch?v=6O6jbZ_fdrY&t=42s

Why worry about engagement?

We want to avoid this sort of situation:

Why provide role-based Information Security Training?

Role-based Information Security Training is important because

- Social engineering of humans is a top threat to information security
- After individual users, system owners, data owners, and others with specific security responsibilities are the next line of defense
- Individuals with specific security responsibilities may not have all the knowledge they need to fulfill these responsibilities
- Targeted, role-based training is more cost-efficient and cost-effective and makes measurable improvements in information security
- Oh, and SEC501 requires it.

Why provide role-based Information Security Training?

So what does SEC501 say about this, anyway?

The organization provides role-based security training to personnel with assigned security roles and responsibilities:

Before authorizing access to the information system or performing assigned duties;

When required by information system changes; and

As practical and necessary thereafter.

Why provide role-based Information Security Training?

OK, I'm with you so far

Tell me more

02 | Making role-based information security training successful

Grouping training for similar roles increases effectiveness

System Owner, Data Owner, and System Administrator roles require similar training

System Owner

- Serve as liaison between IT and business for the system
- Manage system access and training requirements
- Comply with COV and DMV policies and standards
- Work with Data Owner to manage data

Data Owner

- Serve as liaison between IT and business for data
- Determine data sensitivity
- Define data protection requirements
- Work with System Owner to manage data

System Administrator

- Manage and operate the system
- Implement requirements defined by Data and System Owners
- Implement security controls
- Work closely with System and Data Owners

Providing Role-based Information Security Training

To be successful, role-based Information Security training must:

Be tailored to its audience

Be cost-efficient

Be cost-effective

Providing Role-based Information Security Training

To meet these goals we must:

Analyze the audience to determine their training needs

Design training that meets these needs

03 | Analyzing the audience

Analyzing the audience

We're designing training for adult learners who:

Are competent in their regular duties but may not be information security experts

May be resistant to change (there's that bugaboo again)

May fear consequences if they are not successful

Analyzing the audience

Adults who are learning new skills often:

- Don’t want to appear to be beginners
- Dislike looking less than fully competent
- Are unwilling to make mistakes

Using the audience analysis

We can address these concerns by

- Reassuring
- Training
- Coaching
- Supporting

04 | Designing and delivering the training

Designing and delivering the training

We need to provide training that accommodates varied learning styles:

Seeing

Hearing

Reading and Writing

Doing

Training techniques: Video clips

Video clips make great illustrations of the need for information security controls

https://www.youtube.com/watch?v=C4Uc-cztsJo

Training techniques: Video clips

Video clips make great illustrations of the need for information security controls

https://www.youtube.com/watch?v=pQHX-SjgQvQ

Gamification

Game playing is another method of enhancing engagement with training

Security Controls BINGO				
AT-4	CA-6	IR-4	PE-2	AC-22
IA-2	PL-1	AC-1	IR-8	CM-2-COV
AC-17	RA-2	AT-1	PS-1	AT-1
CM-5	MP-4-COV	AC-21-COV	MA-1	CP-3
AU-11	SA-1	SC-5	AC-2	SI-10

Exercises

Exercises work particularly well for those who learning by reading and writing or by doing

Data Type	C	I	A
Customer Name and Address			
Credit Card Number			
Information Security Policies			
Press Releases			
Blog Post			
Medical Records			
Purchasing Invoices			
Email Messages			

Are these systems sensitive for C, I, or A? (could be none or more than one)

DMV CSS

DMV HROS

DGIF Bear Tracking

COV Portfolio Management System

Cardinal

www.virginia.gov

Good Old Presentation/Discussion

Don’t overlook the old standby!

SEC501 Control Families: AC – ACCESS CONTROL

Control	System Owner	Data Owner	System Admin
AC-1 – Access Control Policy and Procedures Develops, documents, and disseminates to all organization personnel, contractors, and service providers with a responsibility to implement access controls an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	Understand org access control policy and procedures	Understand org access control policy and procedures	Understand org access control policy and procedures
	Review and update for their systems P&P on annual basis, or more often if needed	Review and update for their systems P&P on annual basis, or more often if needed	Review and update for their systems P&P on annual basis, or more often if needed
AC-2 – Account Management **AC-2-COV** Identifies and selects the following types of information system accounts to support organizational missions/business functions: individual, group, system, service, application, guest/anonymous, and temporary	Determines types of accounts req'd in system; assigns account mgrs as needed; determines conditions for acct group role and membership; determines who's authorized to use system and privileges they get; notifies AM about changes to accts, e.g., terminations; authorizes access to sys; reviews accounts for compliance annually or as needed; established a process for re-issuing credentials for group accounts	Participates in responsibilities of sys owner as related to access to data	Creates, enables, modifies, disables, and removes information system accounts in accordance with the agency-defined logical access control policy; Monitors the use of information system accounts; and notifies sys owner and data owner and ISRM of anomalies

05 | To conclude . . .

In conclusion

Three takeaways

- Role-based information security training isn't just a requirement. It is
  - Critical to information security
  - A cost-efficient and -effective way to measurably improve security
- The training needs to understand and accommodate varied needs of audience
  - Perspective
  - Learning style
- Role-based information security training can be fun!

Questions and Discussion

Contact Us

Scott Hammer

CISM, CRISC, PMP
Principal Consultant
Commonwealth of Virginia Client Partner

(804) 306-9685
shammer@impactmakers.com

Slide Deck posted at http://www.impactmakers.com/insights/cov-presentations/

06 | Appendix: About Impact Makers

The Impact Makers Difference

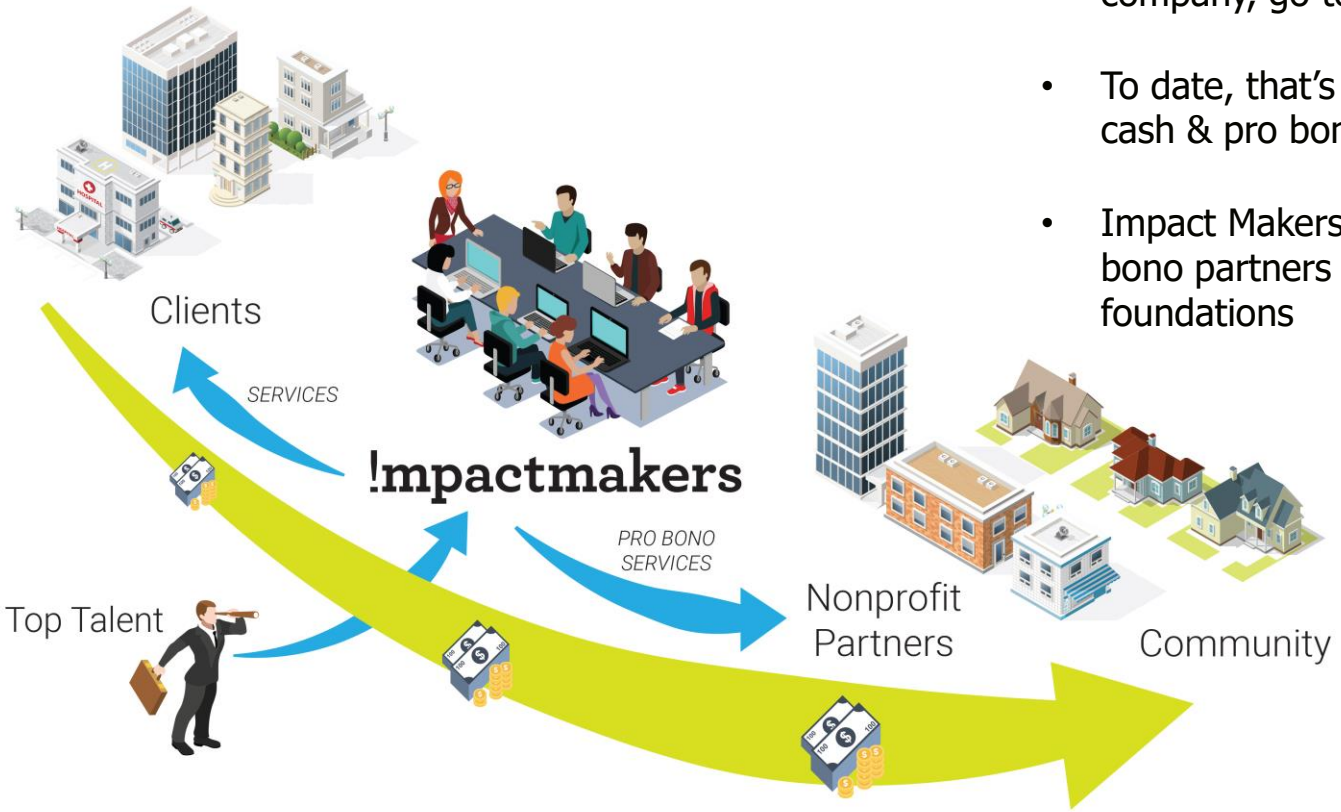
At Impact Makers, we are redefining business.

Our passion is doing the right thing to create meaningful change for our clients and our community.

We drive change through our teams of exceptional people, motivated by our mission and guided by our values.

Achieving success is a different experience with us, by design.

Our Model



*100% of net profits over the life of the company

- 100% of net profits, over the life of the company, go to nonprofit partners
- To date, that's more than $2.5 million in cash & pro bono services
- Impact Makers supports 8 community & pro bono partners and is owned by 2 foundations

How Our Model Benefits Clients

What sets Impact Makers apart and differentiates us as a business is our model. While it is clear why our model matters to our community and employees, it is important to articulate why it should matter to clients.

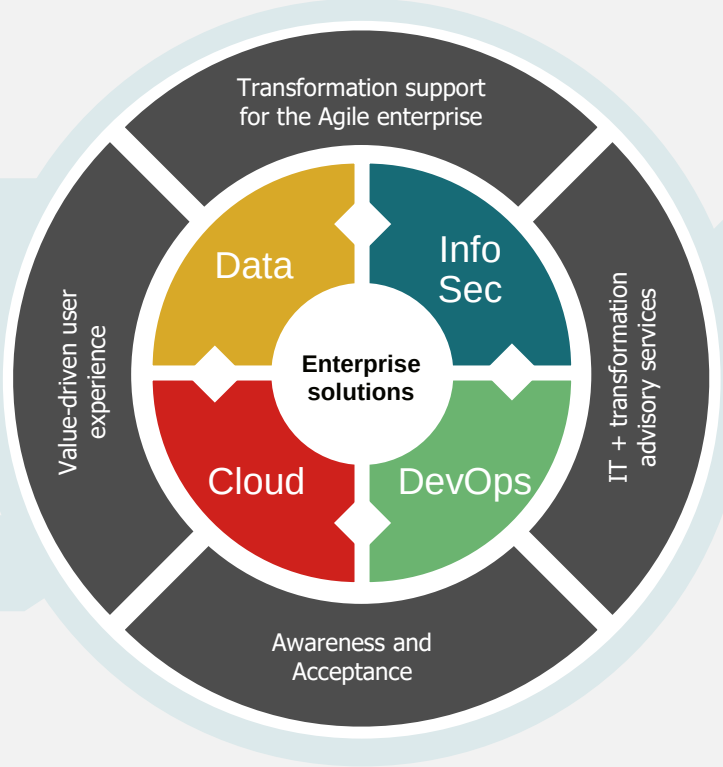
Indicator	Differentiated Benefit to Our Clients
Impact Makers business model attracts phenomenal talent that is driven to make a different for our customers and our communities	!m attracts and retains leaders that others cannot, enabling us to provide clients services and industry best practices
!m's talent acquisition cost is low – referral network and purpose-based draw (70% of hires are referrals)	Bill rates are at a substantive discount for comparable resources with commensurate experience and capabilities when compared with our competitors
Our model serves as grounding for lower turnover and higher retention	Consistency of service, lower disruption
Mission-aligned teams outperform those that are not	Higher productivity and value yield
Ethos that is lived through values and culture	An unmatched level of honesty, transparency and partnership experience

Impact Makers' focus areas

Where we work

- Healthcare payers and providers
- Banking, financial and insurance services
- Public sector

What we do



Why it matters

Together we deliver exceptional results and value

Together we support our community

!m is committed to contributing 100% of net profits to the community over the life of the company.

Examples of Client Work

Impact Makers is delivering transformational strategy and technology programs for large enterprises.

Large Financial Institution

DevOps Managed Service

- Architecting and developing centralized platforms to drive "platform as a service" application migration strategy
- Cloud and automation focus
- 10-person team working across 13 bank divisions
- Tech stack spans Java, .NET, AWS, Azure and a range of CI/CD tools
- Kanban and Agile coaching; velocity-based managed service

M&T Bank

Test Data Governance

- Conducted enterprise-wide analysis to measure risk of a data breach in non-production environments
- Full enterprise mapping to id and analyze all primary systems and environments
- Partnered with risk and compliance to establish test data governance and masking standards
- Architecting data masking solution for core banking systems (Hogan, Shaw)

McKesson

Experience Strategy & Development

- Planned experience design program to increase online revenue and improve marketing team productivity
- Designed and executed primary research strategy with key customers for insights
- Led CMS replatform
- Leading design and build of flagship site
- Integrating & refreshing subsites

Examples of Client Work

Impact Makers is delivering transformational strategy and technology programs for large enterprises.

Transformation & PM Services

$39B+ health care system

- !m facilitated a year-long series of executive meetings to guide leadership through the process of selecting priority projects to help implement their strategic blueprint
- Worked with existing processes and teams to improve core business disciplines such as resource management, risk management and OCM to support not only executive level, but execution teams
- Successfully delivered a detailed strategic blueprint powered by a financial model to translate initiatives into PMPM-level (per member per month) cost savings targets
- And a comprehensive OCM framework, complete with a toolset for activities integrated into a project lifecycle to support the attainment of the company's strategic goals

Information Security Transformation

$3B+ mid-sized health care system

- The client wanted to implement recommendations from a third party IS assessment
- !m analyzed, prioritized and organized the projects into a holistic transformation program
- Identified additional projects necessary to reduce risk
- Delivered a solid foundation for the information security program including frameworks for risk management, security architecture and IS governance
- Developed policies and standards aligned with widely-accepted security controls frameworks
- Piloted a secure texting solution for physicians which ensures HIPAA compliance

Customer Experience

$1B+ mid-sized health care system

- The client sought to develop their customer experience strategy as part of their larger effort to transform their business
- !m performed 18 stakeholder interviews, 48 member and prospect one-on-one interviews, surveys of more than 7,000 members and a facilitated session
- Delivered a CX Strategy and Roadmap the client could start executing immediately
- Identified specific pain points that members experience, along with recommendations
- Recommended 11 key changes to the Member Portal to enhance the customer digital experience
- Built a customer-specific CX Playbook to help the team integrate CX in their product development

Clients

HEALTHCARE

Anthem

Cigna

McKESSON

healthfirst

INOVA HEALTH SYSTEM

PRONTO INSURANCE

BON SECOURS HEALTH SYSTEM

MedStar Health

VCU Health

FINANCIAL

M&T Bank

Freddie Mac

Large Financial Institution

UNION

VIRGINIA DHCD

TAX

GOVERNMENT

VDOT
Virginia Department of Transportation

DMV

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment
www.vdh.virginia.gov

VIRGINIA DEPARTMENT OF SOCIAL SERVICES

Virginia Department of Behavioral Health & Developmental Services

DEPARTMENT OF CORRECTIONS Virginia PUBLIC SAFETY FIRST

VIRGINIA DEPARTMENT OF EDUCATION

VDFP
VIRGINIA DEPARTMENT OF FIRE PROGRAMS

DOA Virginia Department of Accounts

COMMUNITY PARTNERS

Family Lifeline

AHRC new york city

PETER PAUL Development Center

RX PARTNERSHIP
Free Medicine for Virginia's Uninsured

IT4causes

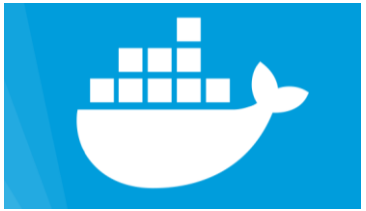
flipm
future leaders in project management

Community OF HOPE

Midwives For Haiti

Technology Partners

Impact Makers aligns technology solutions with our client's needs.



Community Impact

Impact Makers' community contributions are equal to those from multi-billion dollar companies and foundations.

Impact Makers ranked 10th in the 2017 Generosity Inc. Top Richmond Corporate Donors, our 5th year on the list.

1. Altria ($25B)
2. Dominion & Foundation
3. Wells Fargo ($88B)
4. Capital One ($26B)
5. Carmax & Foundation ($15B)
6. TowneBank ($55B)
7. Kroger ($115B)
8. Williams Mullen Foundation
9. Genworth Foundation
10. **Impact Makers ($22.4M)**

Certifications

Impact Makers is proud to be a Founding Certified B Corp, HIMSS Certified Consultant, Certified Small Business and Committed to Recruiting Veterans.

Certified B Corporation

Business as a Force for Good

- Global Movement of 1,200+ Companies
- Certified in 2007

HIMSS Analytics

Certified Consultants

- Valid through December 2019

SWaM-certified Small Business

Virginia Department of Small Business & Supplier Diversity

- #660781
- Valid through December 23, 2019

V3 Certified Company

Virginia Values Veterans

- Committed to recruiting, hiring and retaining Veterans

Awards & Recognition

Impact Makers has made the Inc. 5000 list of fastest growing companies for six consecutive years.

- *Inc.* 5000 Fastest Growing Companies in America – 6 years
- Best for the World & Best for Community – 5 years
- *Fortune* & ICIC Inner City 100 – 3 years
- *Consulting* Seven Small Jewels
- *Richmond Times-Dispatch* Top Workplaces – 4 years
- *Virginia Business* Fantastic 50
- World's Top 25 GameChangers
- *Richmond BizSense* Generosity Inc. Top Corporate Donors – 5 years
- *Consulting* Fastest Growing Firms – ranked 5th in 2016
- *Richmond BizSense* RVA 25 – 4 years