Meeting Member's E-Commerce Demands

How to Make It Easy for Your Members to Do Business With Your Credit Union 24/7

July 20, 2002

Julie J.C.H. Ryan
jjchryan@gwu.edu

First Principles

- What do your members really want?
  - 24/7/365 access to services
  - BUT!
  - Bunch of implied requirements
    - Transaction integrity
    - Data integrity
    - Non-repudiation
    - Availability
    - Confidentiality
- To be successful, they need confidence that…
  - the transaction performed is correct in every way
  - the transaction is not incorrect in any way
  - the service they think they are asking for is in fact the service that is provided

Challenges

- Present a worry free capability that is imbued with all the trust inherent in a conventional banking experience
  - What worries your customers is not always the same thing that worries your security engineers
  - Designing a security solution is complicated by the fact that you have absolutely no control whatsoever over the home computer environment
- Provide an intuitive interface that is:
  - Easy to learn
  - Easy to remember how to use
  - Easy to navigate
  - Easy to use
  - Useful
- Overcome fear of the unknown
  - Technology interface
  - Process elements

Security

- What is security?
  - Webster's: (http://www.m-w.com/cgi-bin/dictionary Sept 24, 2001)
    - Pronunciation: si-'kyur-&-tE
      - Function: noun
      - Inflected Form(s): plural -ties
      - Date: 15th century
    - 1 : the quality or state of being secure : as
      - a : freedom from danger : SAFETY
      - b : freedom from fear or anxiety
      - c : freedom from the prospect of being laid off <job security>
    - 2 a : something given, deposited, or pledged to make certain the fulfillment of an obligation
      - b : SURETY
    - 3 : an evidence of debt or of ownership (as a stock certificate or bond)
    - 4 a : something that secures : PROTECTION
      - b (1) : measures taken to guard against espionage or sabotage, crime, attack, or escape
      - (2) : an organization or department whose task is security

Information Security

- The practice of information security focuses on each of these elements in various means and applications
  - "the quality or state of being secure"
    - Assessing the risk posture of an environment, to include threats, vulnerabilities, and potential impacts
    - Auditing and monitoring the environment against attacks
  - "something given, deposited, or pledged to make certain the fulfillment of an obligation"
    - Access control and mediation; the principle of least privilege
  - "an evidence of debt or of ownership"
    - Identification and authentication, tokens, digital signatures
  - "something that secures : PROTECTION"
    - Focus on the security attributes of information assets and systems
      - Confidentiality, Integrity, Availability
    - Protecting these attributes with technical and management controls

To Simplify

- Providing security of information assets and systems
  - Cannot be done with technology alone
  - Requires on-going analysis and monitoring of the enterprise environment
  - Must be viewed as a composite of these elements:
    - The Risk inherent in the environment
      - Threats, Vulnerabilities, Impact Estimations, Countermeasures
    - Security attributes of the information assets
      - Confidentiality, Integrity, and Availability
    - Policy aspects of the protection framework
      - What needs to be protected? What doesn't?
      - How much protection is needed? What's overkill?
      - How long must the protection be kept in place? How soon can it be released?
    - The phasing of security activities
      - Protection
      - Detection
      - Reaction and Correction

A Word About Threats

- Threats:
  - Natural
    - Fire, Hurricane, Flood, Tornado, etc
  - Malicious
    - Requires both Capability and Intent
      - If no intent, won't act
      - If no capability, can't act
    - Capability
      - Requires both Access and KSA/Tools
        - » If no Access, can't act
        - » If no KSA/Tools, can't act or actions are limited
- This provides a structured way of controlling threat
  - Target intent as much as possible
  - Limit KSA/Tools as much as possible
  - Focus primary efforts on controlling access
    - Both quantity and quality

Security Solutions

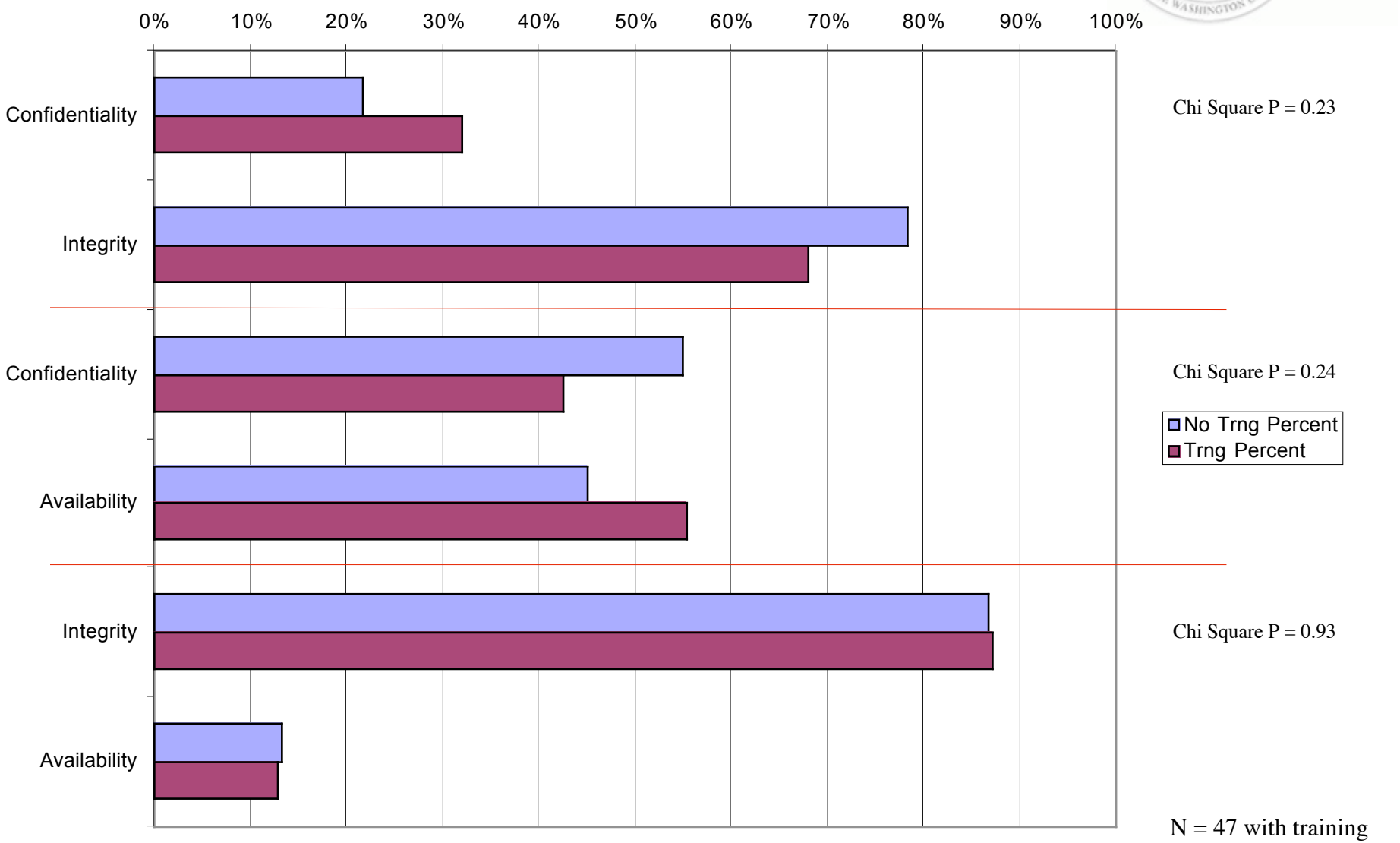
- Security needs to be architected into an environment
  - Architectural approach implies all parts of enterprise environment are considered with regards to the desired solution space
    - Physical security
      - "guards, gates, locks" but also the entire practices of facilities security
    - Computer security
      - Secure computing approaches, configuration management, access control
    - Network security
      - Controlled and monitored networking connections, access control
    - Personnel security
      - Understanding who you are letting into your environment, access control
    - Operational security
      - Holistic security approach to operational environment, processes, procedures
  - Focus is to limit threat access, mitigate vulnerabilities, distribute impact, and manage risk

Worries, Part 1

- Your members don't want to be exposed to insecurity
  - They don't want to be afraid
- Security attributes of the data and the transactions
  - Confidentiality
    - Of the data
    - Of the transactions
  - Integrity
    - Of the data
    - Of the transactions
  - Availability
    - Of data
    - Of transactions

What is Most Important?

Percentages Comparison -- Training Question

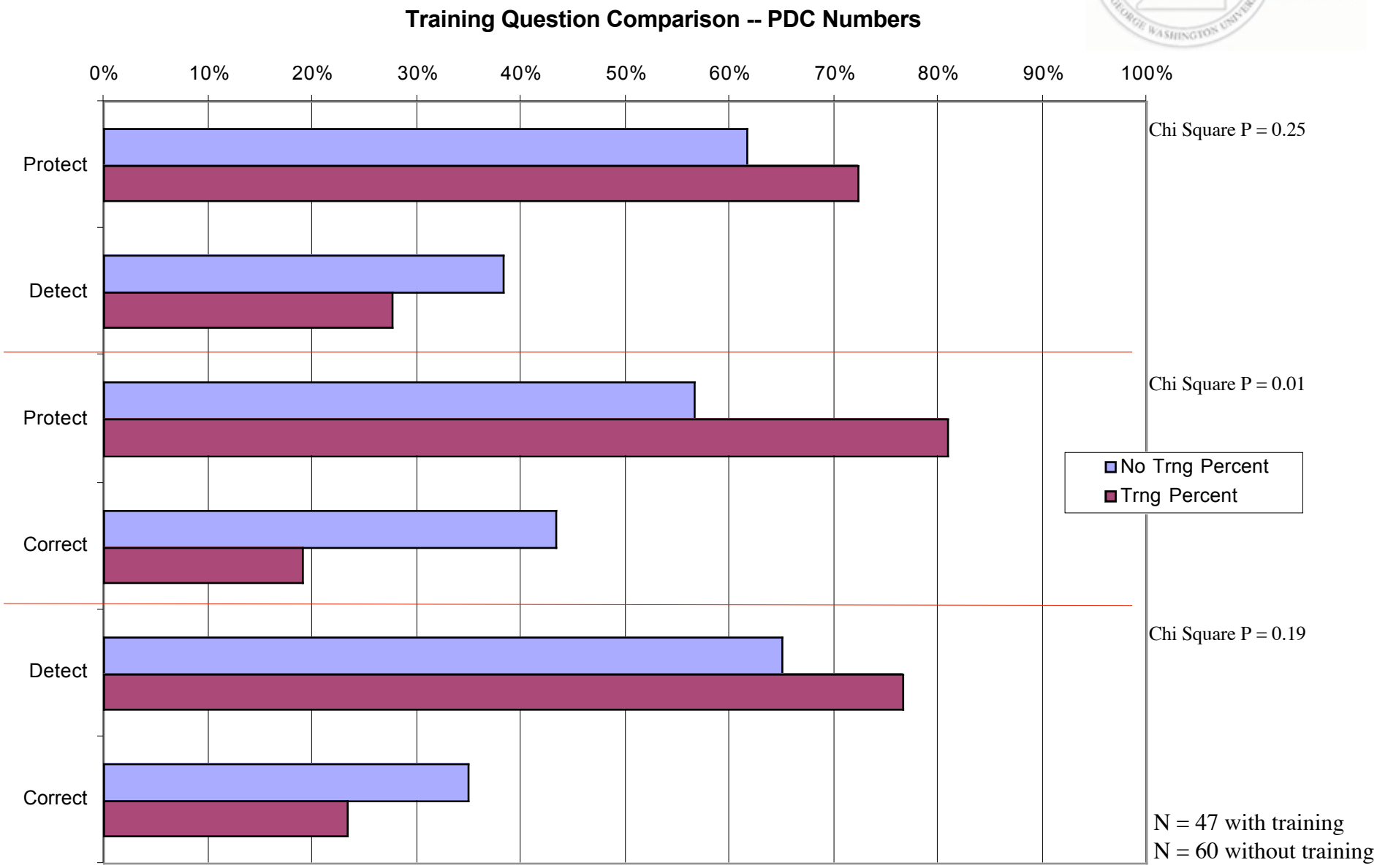


N = 47 with training
N = 60 without training

Worries, Part 2

- Adequate protections
  - For the confidentiality, integrity and availability
  - Of data and transactions
  - With limited resources
- The ability to fix things when they go wrong
  - The ability to detect when problems occur or security mechanisms fail
    - For problems that are protected against
    - For problems that are not protected against
    - For problems that were not considered or known about
    - For malicious activity that is stealthy in nature
  - The resources and capabilities to react and correct any problem situation that occurs
    - With adequate assurance that the reaction is correct
    - In a timely manner
    - With comprehensive solutions

Protect, Detect, Correct



Solution to Worries

- Security managed through limitations on functionality
  - Can't control home computing environment, so therefore must assume malicious end user activity
  - Limiting functionality constrains capabilities of attackers
- Identifying and authenticating end users problematic
  - Passwords are cheap and easy, but a problem waiting to happen
    - Compromised passwords, forgotten passwords, easy to guess passwords
    - How many passwords do you have to how many systems?
  - Consider using a one-time password solution
    - May seem more costly, but life-cycle costs may actually be less depending on the size and complexity of the user population
- Continually reinforce the message of security to your user population
  - Make sure you're doing it right
  - Take away the concerns of your members

The Interface Issue

- Overly complex systems are a barrier to use
  - Human-computer interaction design principles can assist
  - Should be integrated tightly with security engineering goals
- Consider the ATM
  - Extremely limited functionality with narrow range of choices….
  - Anyone ever get confused over which choice to pick?
    - Which type of account?
    - Which account number?
  - Ever go to a different ATM than you normally use and get confused because the interface is different?
- Providing an interface that is easily interpreted, easily manipulated, and easily navigated is absolutely critical
  - For all ages, for all cultures, for all educational backgrounds
  - Colors, symbols, size, font types, etc all have emotional meaning

HCI Engineering

- Interface should have these qualities
  - Easy to learn
  - Easy to remember how to use
  - Easy to navigate
  - Easy to use
  - Useful
- Consider using a metaphor in your interface design
  - Take a physical bank and reproduce it conceptually
  - Make sure you aren't making assumptions about knowledge or expectations
    - Testing on real users helps identify shortcomings in this arena
  - Use "normal" technology interfaces if possible
    - Web-like interface stripped of extraneous capability and enabled by cryptography can provide a comfortable mental experience
  - Train your users by adopting elements of the interface in marketing, promotional, and communications materials

Fear of the Unknown

- Getting customers to adopt a new technology can be difficult
  - Especially if they are afraid of it and what it can do
    - Can they figure it out?
    - Can they use it successfully?
    - Can their accounts be hacked?
    - Can someone steal all their money?
- Integrating the capability into normal operations eases those fears by making the capability familiar
  - Treat it as normal, and very cool
  - Show full confidence in the security features
  - Provide easy to understand user guides
  - Make sure the home computer software installation is absolutely brainless
  - At first, have extra staff on hand to ease the transition
    - Help desk
    - On-site demonstration capabilities

The Bottom Line

- Making it easy for your members requires a lot of up-front engineering and design thought
  - Security engineering
  - Useability engineering
  - Normalization of capabilities
- If you do it right, it will be so easy as to be trivial
  - It will become an expected component that is noticeably by its absence
- If you do it wrong….
  - Low adoption rate of the capability
    - ROI…..
  - Your members will be unhappy
  - Potentially expose the credit union to more risk than necessary

Contact Information

Julie J.C.H. Ryan, D.Sc.
1776 G. Street NW #101
Washington DC, 20052
jjchryan@gwu.edu
http://www.seas.gwu.edu/~infosec/

The George Washington University is an NSA Certified Center of Academic Excellence in Information Assurance Education and meets the Federal Training Standards for Information Systems Security Professionals (NSTISSI 4011). We offer Graduate Certificate, Master's, and Doctoral level education in Information Security Management for professionals from all educational backgrounds. GWU is located in the heart of Washington DC very near the White House and other government offices.