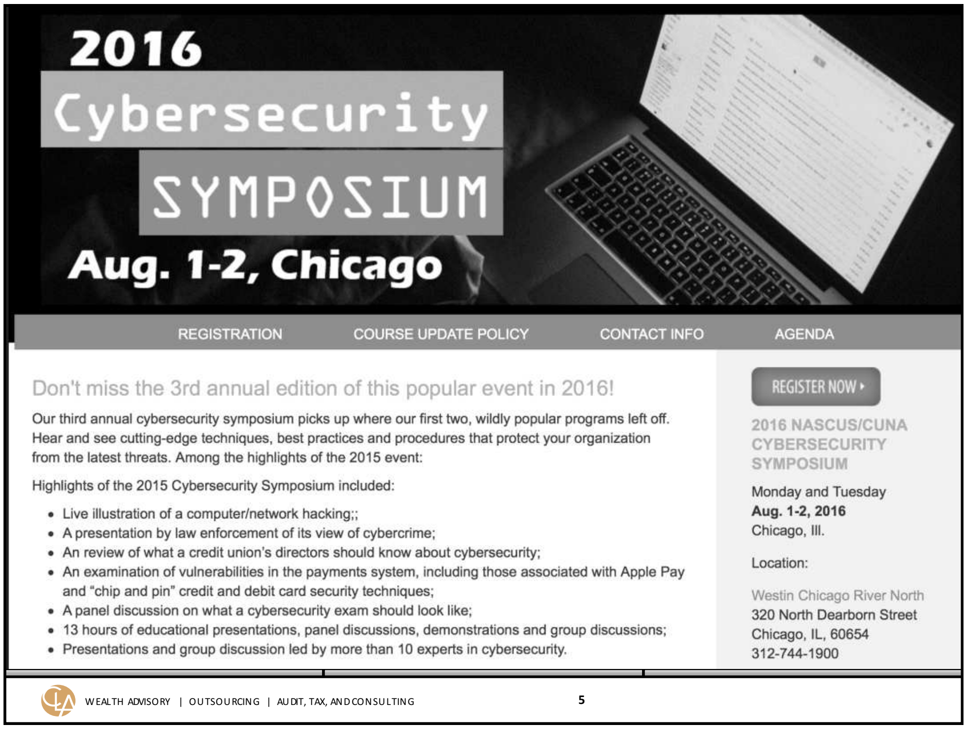
Risk Assessment and other Defensive Security Measures

Tom Schauer – Principal
CISA, CISM, CISSP, CEH, CRISC, CTGA
CliftonLarsonAllen - Information Security Services Group



2016 Cybersecurity SYMPOSIUM Aug. 1-2, Chicago

Don't miss the 3rd annual edition of this popular event in 2016!

Our third annual cybersecurity symposium picks up where our first two, wildly popular programs left off. Hear and see cutting-edge techniques, best practices and procedures that protect your organization from the latest threats. Among the highlights of the 2015 event:

Highlights of the 2015 Cybersecurity Symposium included:

- Live illustration of a computer/network hacking;;
- A presentation by law enforcement of its view of cybercrime;
- An review of what a credit union's directors should know about cybersecurity;
- An examination of vulnerabilities in the payments system, including those associated with Apple Pay and "chip and pin" credit and debit card security techniques;
- A panel discussion on what a cybersecurity exam should look like;
- 13 hours of educational presentations, panel discussions, demonstrations and group discussions;
- Presentations and group discussion led by more than 10 experts in cybersecurity.

2016 NASCUS/CUNA CYBERSECURITY SYMPOSIUM

Monday and Tuesday
Aug. 1-2, 2016
Chicago, Ill.

Location:

Westin Chicago River North
320 North Dearborn Street
Chicago, IL, 60654
312-744-1900

Fun SE Stories

- Beth really wanted her Starbucks. Clicked 6 times.
- Begged to know, “Are you tricking me?”
- Came back to the office to restart payload.
- Actually tried to repair the copier.

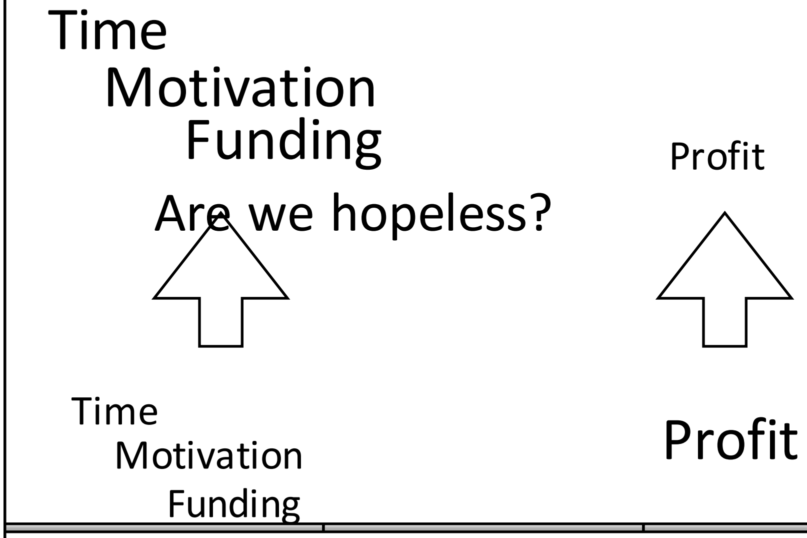
"In the world of networked computers every sociopath is your neighbor“ …Dan Geer

The Threatscape We Now Face…

"The threat has reached the point that, given enough time, motivation, and funding, a determined adversary will likely be able to penetrate any system accessible from the Internet."

Joseph M Demarest, Assistant Director, Cyber Division FBI, before the Senate Judiciary Committee, May 8, 2013

This is your security program!



Time
Motivation
Funding

Profit

Are we hopeless?

Time
Motivation
Funding

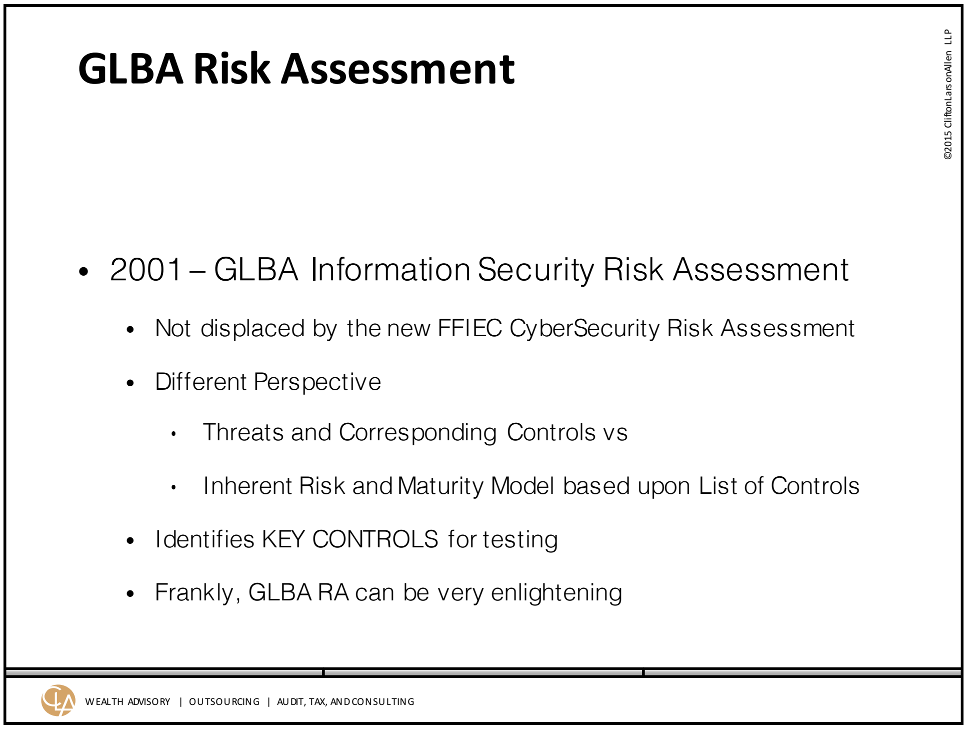
Profit

Key Action

- Risk Assessment
  - Only as good as the effort put into it.
  - Must be championed from the top and not just a check box for exam preparation
  - Risk changes and threats change – cannot be static

Risk Assessment

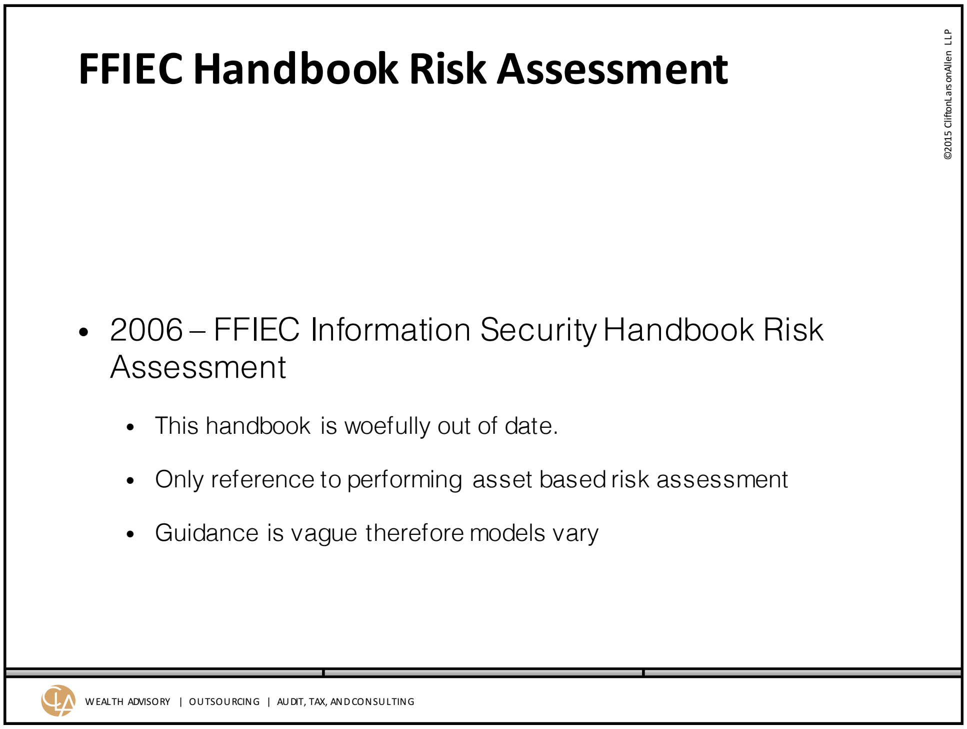
- 2001 – GLBA Information Security Risk Assessment
- 2006 – FFIEC Information Security Risk Assessment
- 2010 - Online Banking Authentication Risk Assessment
- mid-2010s – Social Media and DDoS Risk Assessments
- 2015 – FFIEC CyberSecurity Risk Assessment



GLBA Risk Assessment

- 2001 – GLBA Information Security Risk Assessment
  - Not displaced by the new FFIEC CyberSecurity Risk Assessment
  - Different Perspective
    - Threats and Corresponding Controls vs
    - Inherent Risk and Maturity Model based upon List of Controls
  - Identifies KEY CONTROLS for testing
  - Frankly, GLBA RA can be very enlightening

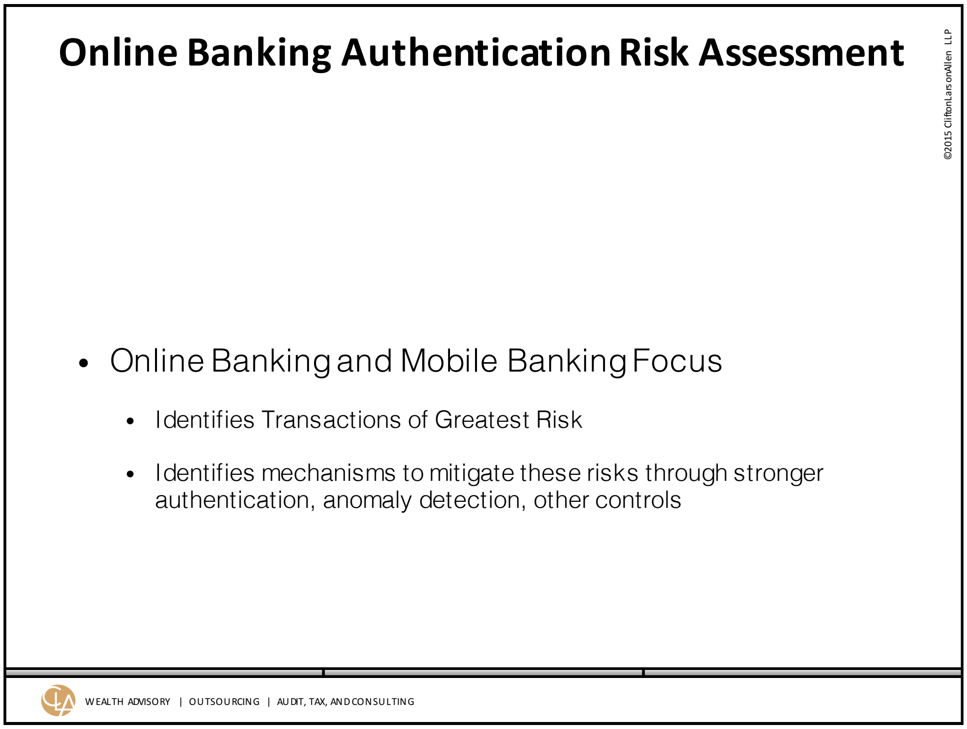
WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



FFIEC Handbook Risk Assessment

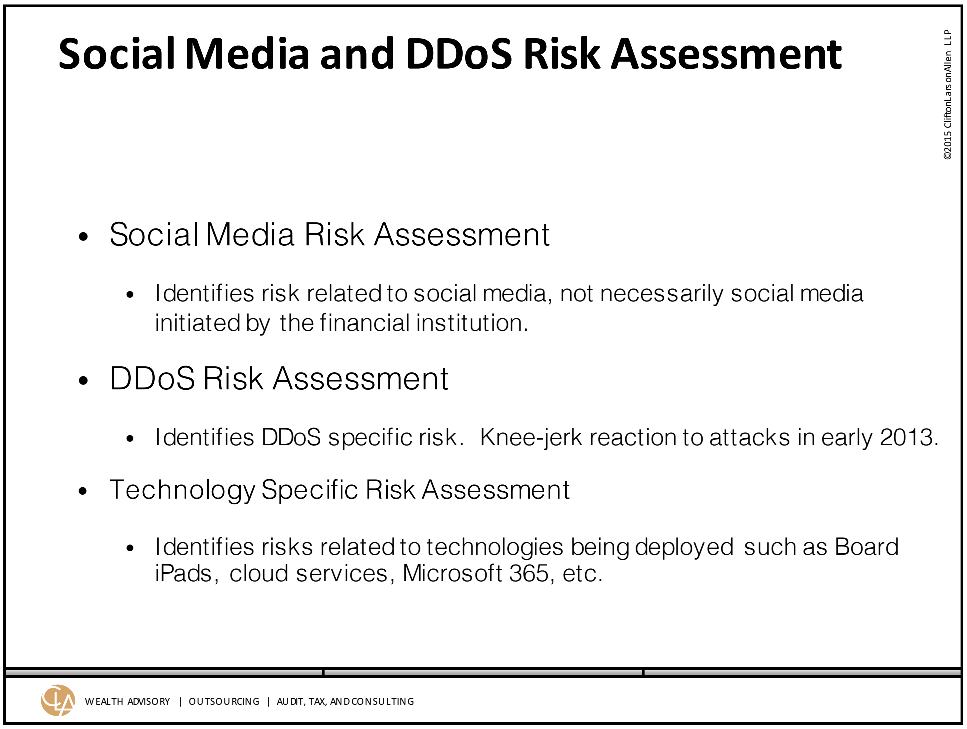
- 2006 – FFIEC Information Security Handbook Risk Assessment
  - This handbook is woefully out of date.
  - Only reference to performing asset based risk assessment
  - Guidance is vague therefore models vary

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



Online Banking Authentication Risk Assessment

- Online Banking and Mobile Banking Focus
  - Identifies Transactions of Greatest Risk
  - Identifies mechanisms to mitigate these risks through stronger authentication, anomaly detection, other controls



Social Media and DDoS Risk Assessment

- Social Media Risk Assessment
  - Identifies risk related to social media, not necessarily social media initiated by the financial institution.
- DDoS Risk Assessment
  - Identifies DDoS specific risk. Knee-jerk reaction to attacks in early 2013.
- Technology Specific Risk Assessment
  - Identifies risks related to technologies being deployed such as Board iPads, cloud services, Microsoft 365, etc.

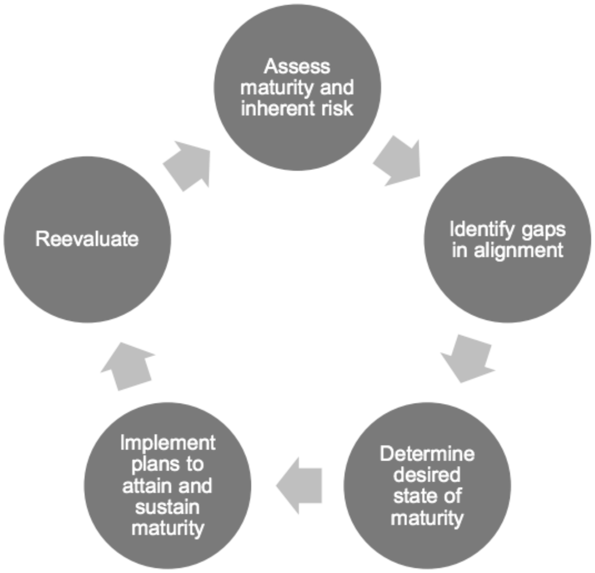
FFIEC Cybersecurity Self Assessment

- Two years in development!
- Initially labeled as Voluntary…
- Voluntary verbiage is removed… not mandatory.
- Will be an examination tool

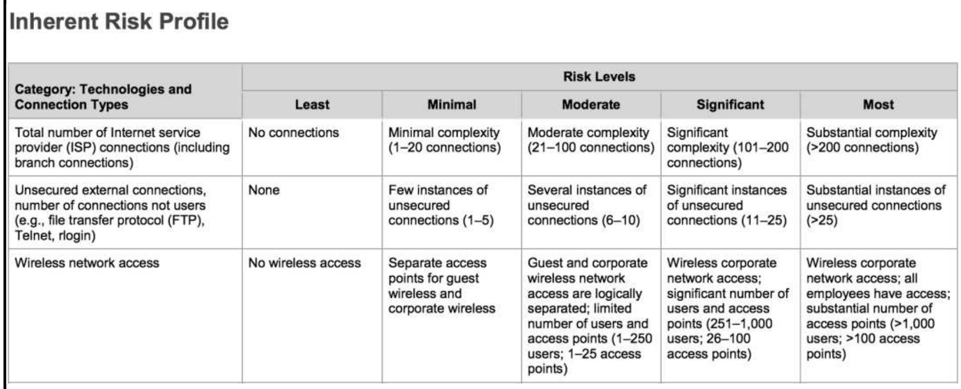
FFIEC Cybersecurity Self Assessment

- Benefits to Institution and Board
  - Consistent evaluation
  - Know your risks
  - Develop a Plan
  - Measure over Time
- Challenges
  - Only as good as the effort/critical thought put into it.
- Two Components: Inherent Risk, Maturity

FFIEC Cybersecurity Self Assessment


Assess maturity and inherent risk
Identify gaps in alignment
Determine desired state of maturity
Implement plans to attain and sustain maturity
Reevaluate

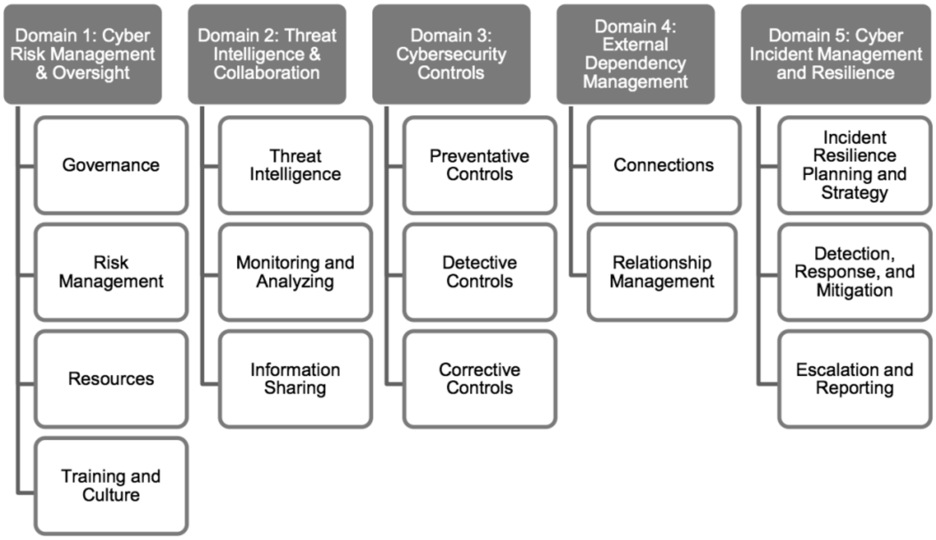
FFIEC Cybersecurity Self Assessment



Inherent Risk Profile

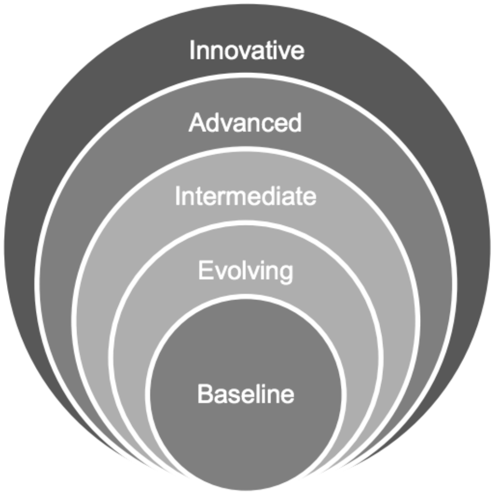
Category: Technologies and Connection Types	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Total number of Internet service provider (ISP) connections (including branch connections)	No connections	Minimal complexity (1–20 connections)	Moderate complexity (21–100 connections)	Significant complexity (101–200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	None	Few instances of unsecured connections (1–5)	Several instances of unsecured connections (6–10)	Significant instances of unsecured connections (11–25)	Substantial instances of unsecured connections (>25)
Wireless network access	No wireless access	Separate access points for guest wireless and corporate wireless	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points)	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points)	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points)

FFIEC Cybersecurity Self Assessment



- Domain 1: Cyber Risk Management & Oversight
  - Governance
  - Risk Management
  - Resources
  - Training and Culture
- Domain 2: Threat Intelligence & Collaboration
  - Threat Intelligence
  - Monitoring and Analyzing
  - Information Sharing
- Domain 3: Cybersecurity Controls
  - Preventative Controls
  - Detective Controls
  - Corrective Controls
- Domain 4: External Dependency Management
  - Connections
  - Relationship Management
- Domain 5: Cyber Incident Management and Resilience
  - Incident Resilience Planning and Strategy
  - Detection, Response, and Mitigation
  - Escalation and Reporting

FFIEC Cybersecurity Self Assessment



Innovative

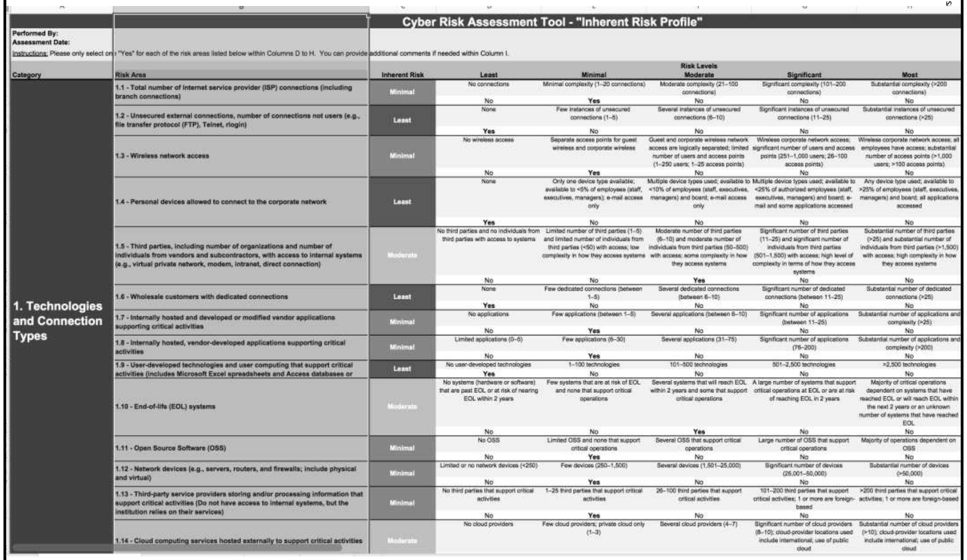
Advanced

Intermediate

Evolving

Baseline

WEALTH ADVISOR



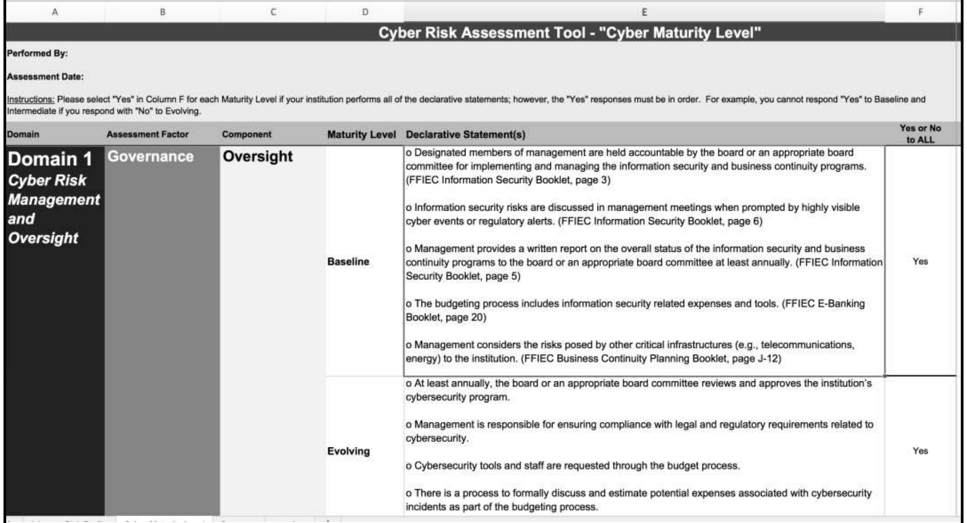
Cyber Risk Assessment Tool - "Inherent Risk Profile"

Performed By:
Assessment Date:

Instructions: Please only select one "Yes" for each of the risk areas listed below within Columns D to H. You can provide additional comments if needed within Column I.

					Risk Levels		
Category	**Risk Area**	**Inherent Risk**	**Least**	**Minimal**	**Moderate**	**Significant**	**Most**
1. Technologies and Connection Types	1.1 - Total number of Internet service provider (ISP) connections (including branch connections)	Minimal	No connections No	Minimal complexity (1–20 connections) **Yes**	Moderate complexity (21–100 connections) No	Significant complexity (101–200 connections) No	Substantial complexity (>200 connections) No
	1.2 - Unsecured external connections, number of connections not users (e.g., file transfer protocol (FTP), Telnet, rlogin)	Least	None **Yes**	Few instances of unsecured connections (1–5) No	Several instances of unsecured connections (6–10) No	Significant instances of unsecured connections (11–25) No	Substantial instances of unsecured connections (>25) No
	1.3 - Wireless network access	Minimal	No wireless access No	Separate access points for guest wireless and corporate wireless **Yes**	Guest and corporate wireless network access are logically separated; limited number of users and access points (1–250 users; 1–25 access points) No	Wireless corporate network access; significant number of users and access points (251–1,000 users; 26–100 access points) No	Wireless corporate network access; all employees have access; substantial number of access points (>1,000 users; >100 access points) No
	1.4 - Personal devices allowed to connect to the corporate network	Least	None **Yes**	Only one device type available; available to <5% of employees (staff, executives, managers); e-mail access only No	Multiple device types used; available to <10% of employees (staff, executives, managers) and board; e-mail access only No	Multiple device types used; available to <25% of authorized employees (staff, executives, managers) and board; e-mail and some applications accessed No	Any device type used; available to >25% of employees (staff, executives, managers) and board; all applications accessed No
	1.5 - Third parties, including number of organizations and number of individuals from vendors and subcontractors, with access to internal systems (e.g., virtual private network, modem, intranet, direct connection)	Moderate	No third parties and no individuals from third parties with access to systems No	Limited number of third parties (1–5) and limited number of individuals from third parties (<50) with access; low complexity in how they access systems No	Moderate number of third parties (6–10) and moderate number of individuals from third parties (50–500) with access; some complexity in how they access systems **Yes**	Significant number of third parties (11–25) and significant number of individuals from third parties (501–1,500) with access; high level of complexity in terms of how they access systems No	Substantial number of third parties (>25) and substantial number of individuals from third parties (>1,500) with access; high complexity in how they access systems No
	1.6 - Wholesale customers with dedicated connections	Least	None **Yes**	Few dedicated connections (between 1–5) No	Several dedicated connections (between 6–10) No	Significant number of dedicated connections (between 11–25) No	Substantial number of dedicated connections (>25) No
	1.7 - Internally hosted and developed or modified vendor applications supporting critical activities	Minimal	No applications No	Few applications (between 1–5) **Yes**	Several applications (between 6–10) No	Significant number of applications (between 11–25) No	Substantial number of applications and complexity (>25) No
	1.8 - Internally hosted, vendor-developed applications supporting critical activities	Minimal	Limited applications (0–5) No	Few applications (6–30) **Yes**	Several applications (31–75) No	Significant number of applications (76–200) No	Substantial number of applications and complexity (>200) No
	1.9 - User-developed technologies and user computing that support critical activities (includes Microsoft Excel spreadsheets and Access databases or	Least	No user-developed technologies **Yes**	1–100 technologies No	101–500 technologies No	501–2,500 technologies No	>2,500 technologies No
	1.10 - End-of-life (EOL) systems	Moderate	No systems (hardware or software) that are past EOL or at risk of nearing EOL within 2 years No	Few systems that are at risk of EOL and none that support critical operations No	Several systems that will reach EOL within 2 years and some that support critical operations **Yes**	A large number of systems that support critical operations at EOL or are at risk of reaching EOL in 2 years No	Majority of critical operations dependent on systems that have reached EOL or will reach EOL within the next 2 years or an unknown number of systems that have reached EOL No
	1.11 - Open Source Software (OSS)	Minimal	No OSS No	Limited OSS and none that support critical operations **Yes**	Several OSS that support critical operations No	Large number of OSS that support critical operations No	Majority of operations dependent on OSS No
	1.12 - Network devices (e.g., servers, routers, and firewalls; include physical and virtual)	Minimal	Limited or no network devices (<250) No	Few devices (250–1,500) **Yes**	Several devices (1,501–25,000) No	Significant number of devices (25,001–50,000) No	Substantial number of devices (>50,000) No
	1.13 - Third-party service providers storing and/or processing information that support critical activities (Do not have access to internal systems, but the institution relies on their services)	Minimal	No third parties that support critical activities No	1–25 third parties that support critical activities **Yes**	26–100 third parties that support critical activities No	101–200 third parties that support critical activities; 1 or more are foreign-based No	>200 third parties that support critical activities; 1 or more are foreign-based No
	1.14 - Cloud computing services hosted externally to support critical activities	Moderate	No cloud providers	Few cloud providers; private cloud only (1–3)	Several cloud providers (4–7)	Significant number of cloud providers (8–10); cloud-provider locations used include international; use of public cloud	Substantial number of cloud providers (>10); cloud-provider locations used include international; use of public cloud

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



Cyber Risk Assessment Tool - "Cyber Maturity Level"

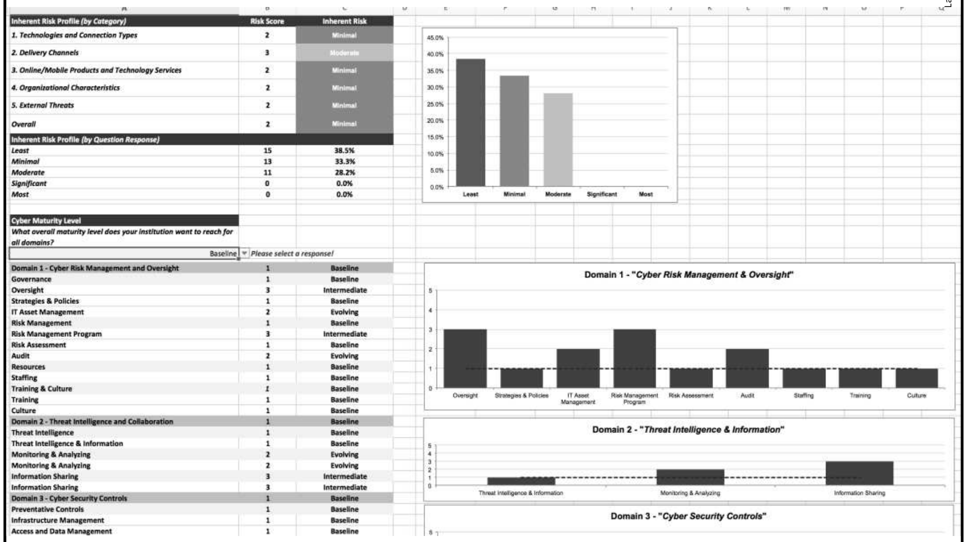
Performed By:

Assessment Date:

Instructions: Please select "Yes" in Column F for each Maturity Level if your institution performs all of the declarative statements; however, the "Yes" responses must be in order. For example, you cannot respond "Yes" to Baseline and Intermediate if you respond with "No" to Evolving.

Domain	Assessment Factor	Component	Maturity Level	Declarative Statement(s)	Yes or No to ALL
Domain 1 ***Cyber Risk Management and Oversight***	**Governance**	**Oversight**	**Baseline**	o Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3) o Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6) o Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5) o The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20) o Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, page J-12)	Yes
			Evolving	o At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program. o Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity. o Cybersecurity tools and staff are requested through the budget process. o There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	Yes

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

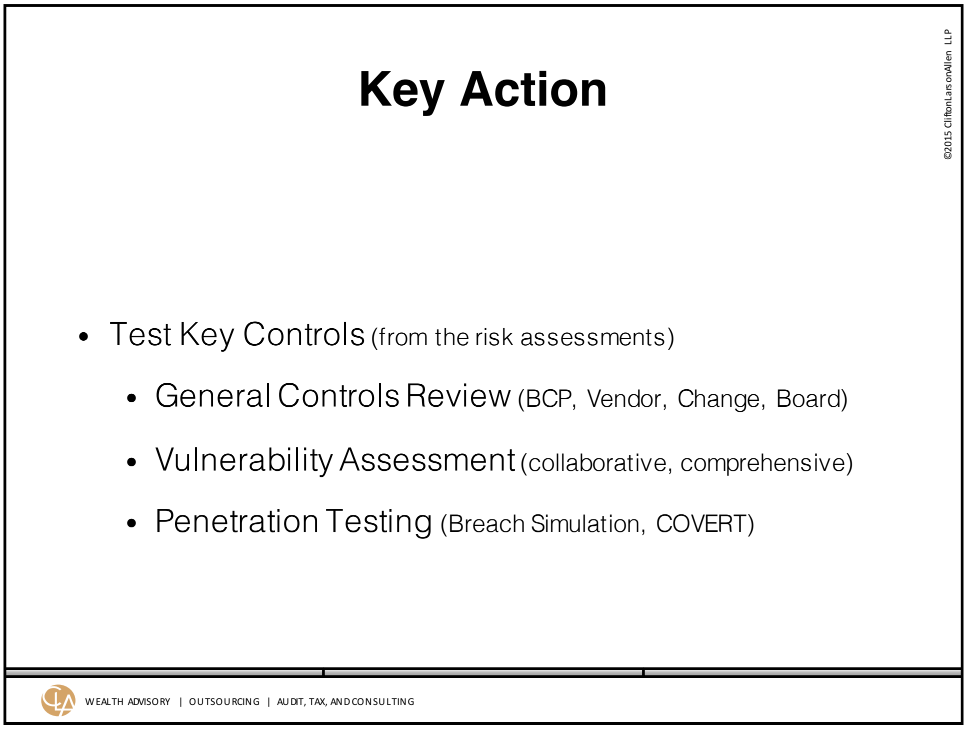


Inherent Risk Profile *(by Category)*	Risk Score	Inherent Risk
1. Technologies and Connection Types	2	Minimal
2. Delivery Channels	3	Moderate
3. Online/Mobile Products and Technology Services	2	Minimal
4. Organizational Characteristics	2	Minimal
5. External Threats	2	Minimal
Overall	2	Minimal
Inherent Risk Profile *(by Question Response)*		
Least	15	38.5%
Minimal	13	33.3%
Moderate	11	28.2%
Significant	0	0.0%
Most	0	0.0%
Cyber Maturity Level		
What overall maturity level does your institution want to reach for all domains?		
Baseline	*Please select a response!*	
Domain 1 - Cyber Risk Management and Oversight	1	Baseline
Governance	1	Baseline
Oversight	3	Intermediate
Strategies & Policies	1	Baseline
IT Asset Management	2	Evolving
Risk Management	1	Baseline
Risk Management Program	3	Intermediate
Risk Assessment	1	Baseline
Audit	2	Evolving
Resources	1	Baseline
Staffing	1	Baseline
Training & Culture	1	Baseline
Training	1	Baseline
Culture	1	Baseline
Domain 2 - Threat Intelligence and Collaboration	1	Baseline
Threat Intelligence	1	Baseline
Threat Intelligence & Information	1	Baseline
Monitoring & Analyzing	2	Evolving
Monitoring & Analyzing	2	Evolving
Information Sharing	3	Intermediate
Information Sharing	3	Intermediate
Domain 3 - Cyber Security Controls	1	Baseline
Preventative Controls	1	Baseline
Infrastructure Management	1	Baseline
Access and Data Management	1	Baseline

LarsonAllen LLP

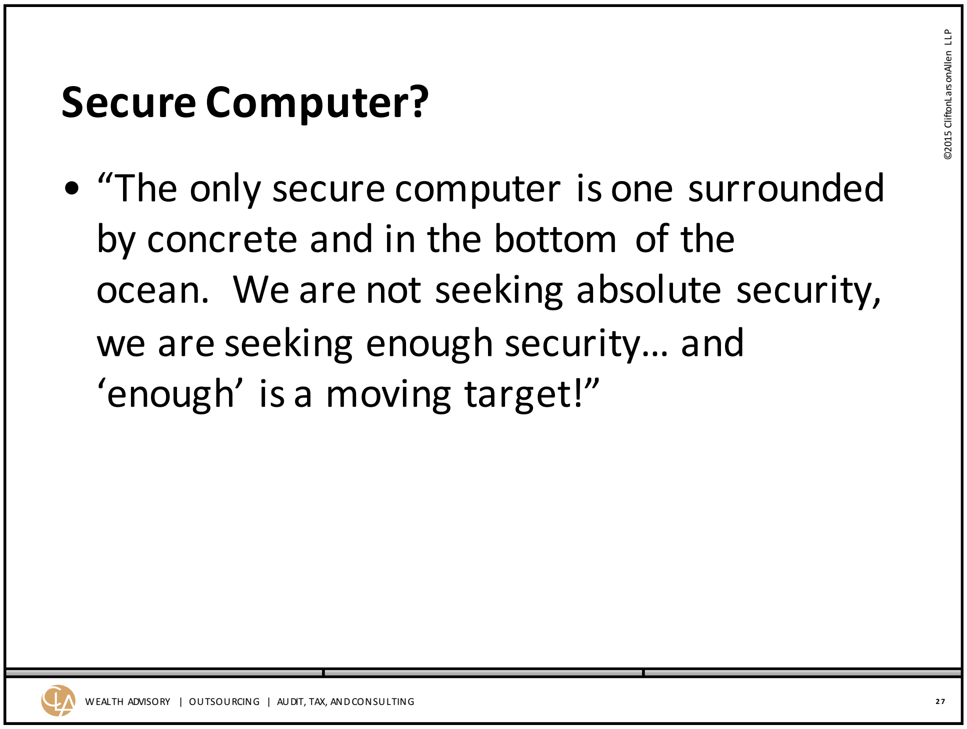
Risk Assessment Wrap Up

- Combined, the CyberSecurity and GLBA Risk Assessment will help you be well informed.
- Having your controls independently tested will validate your risk assessments.
- Well Informed + Validated = Good Decisions



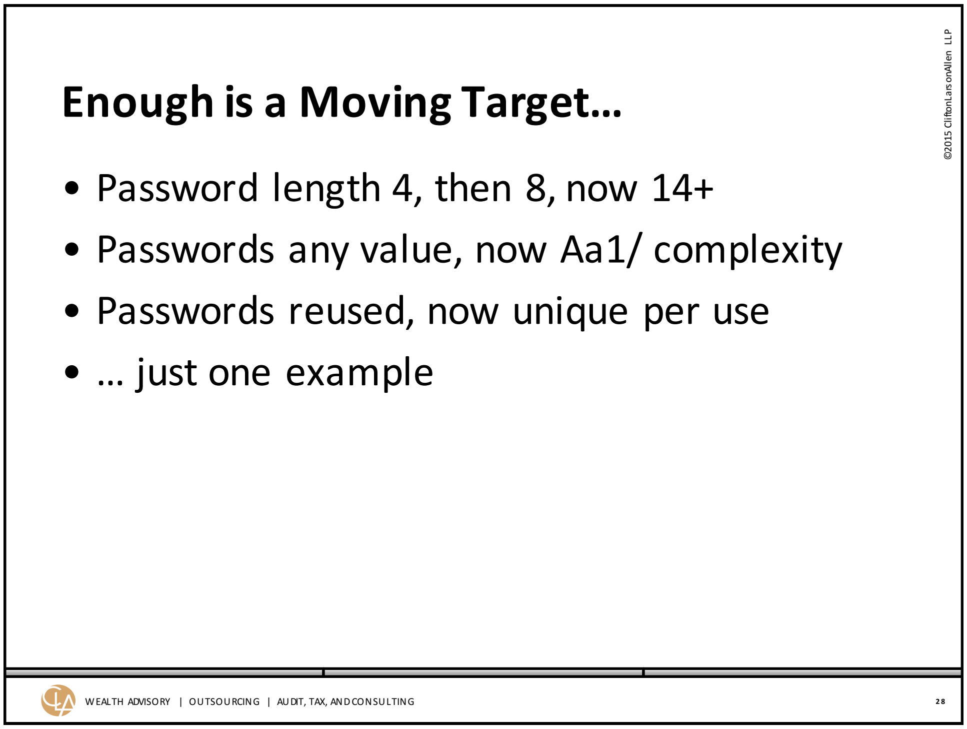
Key Action

- Test Key Controls (from the risk assessments)
  - General Controls Review (BCP, Vendor, Change, Board)
  - Vulnerability Assessment (collaborative, comprehensive)
  - Penetration Testing (Breach Simulation, COVERT)



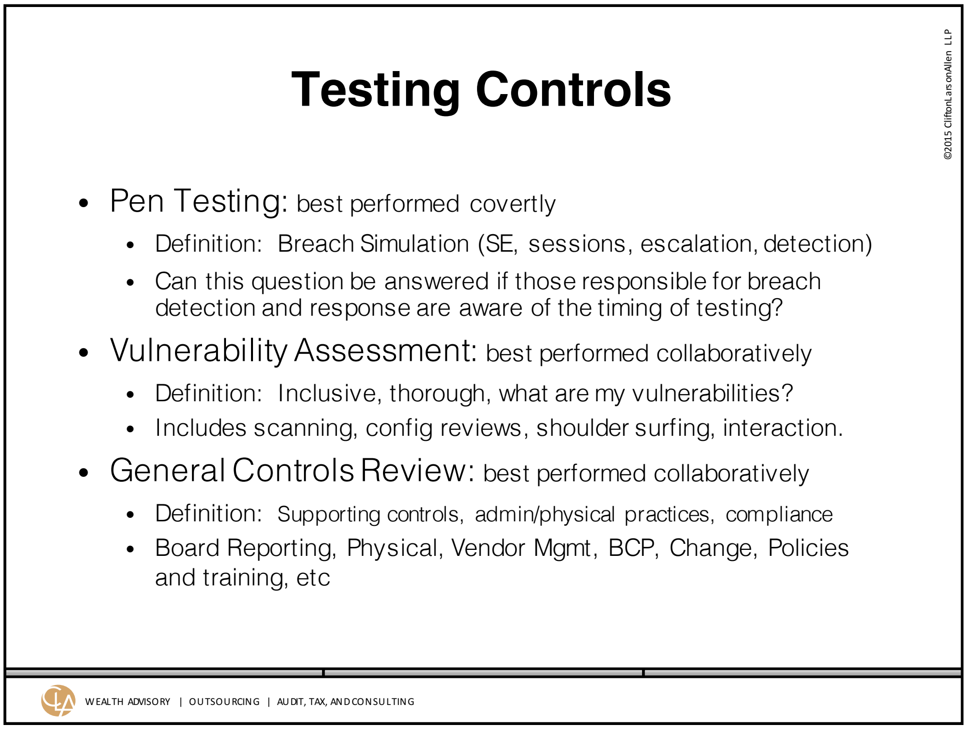
Secure Computer?

- “The only secure computer is one surrounded by concrete and in the bottom of the ocean. We are not seeking absolute security, we are seeking enough security… and ‘enough’ is a moving target!”



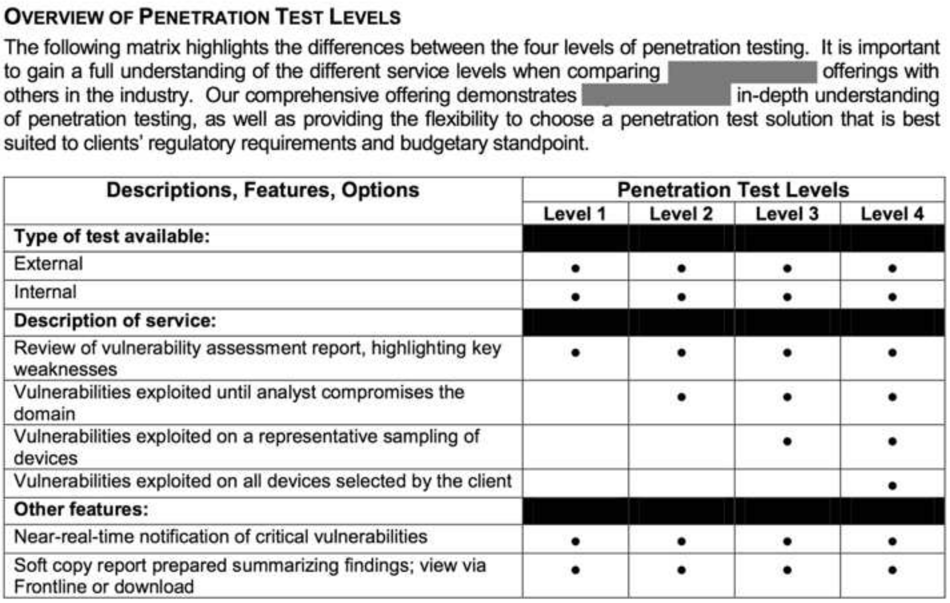
Enough is a Moving Target…

- Password length 4, then 8, now 14+
- Passwords any value, now Aa1/ complexity
- Passwords reused, now unique per use
- … just one example



Testing Controls

- Pen Testing: best performed covertly
  - Definition: Breach Simulation (SE, sessions, escalation, detection)
  - Can this question be answered if those responsible for breach detection and response are aware of the timing of testing?
- Vulnerability Assessment: best performed collaboratively
  - Definition: Inclusive, thorough, what are my vulnerabilities?
  - Includes scanning, config reviews, shoulder surfing, interaction.
- General Controls Review: best performed collaboratively
  - Definition: Supporting controls, admin/physical practices, compliance
  - Board Reporting, Physical, Vendor Mgmt, BCP, Change, Policies and training, etc



Overview of Penetration Test Levels

The following matrix highlights the differences between the four levels of penetration testing. It is important to gain a full understanding of the different service levels when comparing [redacted] offerings with others in the industry. Our comprehensive offering demonstrates [redacted] in-depth understanding of penetration testing, as well as providing the flexibility to choose a penetration test solution that is best suited to clients' regulatory requirements and budgetary standpoint.

Descriptions, Features, Options	Penetration Test Levels			
	Level 1	Level 2	Level 3	Level 4
Type of test available:				
External	•	•	•	•
Internal	•	•	•	•
Description of service:				
Review of vulnerability assessment report, highlighting key weaknesses	•	•	•	•
Vulnerabilities exploited until analyst compromises the domain		•	•	•
Vulnerabilities exploited on a representative sampling of devices			•	•
Vulnerabilities exploited on all devices selected by the client				•
Other features:				
Near-real-time notification of critical vulnerabilities	•	•	•	•
Soft copy report prepared summarizing findings; view via Frontline or download	•	•	•	•

"True Breach Simulation"

- Almost 90% of "real attacks" start with social engineering to obtain network access, then establish persistence, carefully escalate access and privileges, commit fraud or data theft…

- Effective Pen-testing mirrors this approach and is done **without IT knowledge!**
- This is separate from collaborative testing.
- Results: 65% / 100% Compromise

Bears….

- “When you and a friend are being chased by a bear, it is not necessary to out run the bear, it is only necessary to out run your friend.”
- Effective security **May Be** nothing more than being more secure than the FI down the road?

Are you Ready for Breach?

- Would your IT detect a breach? Are you sure?
  - Our IT is REALLY GOOD!
  - Our IS&T Exam was clean!
  - Our security partner scans our systems!
  - We subject our personnel and IT to “True Breach Simulation” and they’ve gotten good and breach avoidance, detection and response!

Breach Preparedness

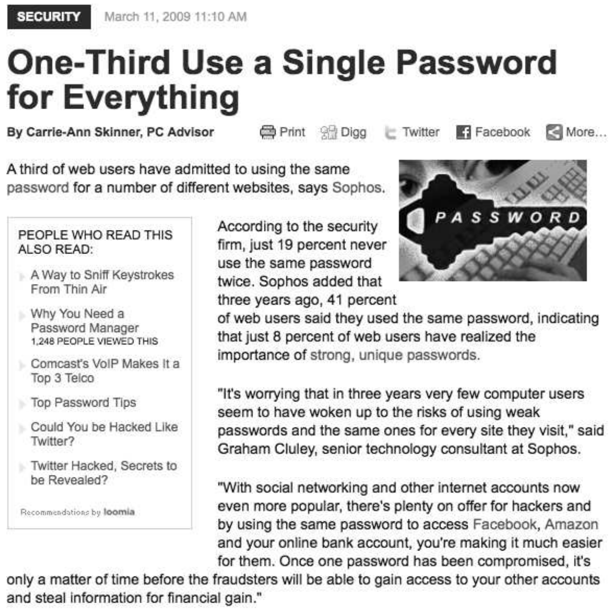
- CyberSecurity Insurance Review
- Security Testing and Remediation
- Legal Preparedness
- Public Relations Preparedness

- A BREACH COACH with your interests in mind!

Now…

- Practical Guidance

Single biggest lesson for today, complex, unique, varied passwords!



SECURITY March 11, 2009 11:10 AM

One-Third Use a Single Password for Everything

By Carrie-Ann Skinner, PC Advisor

A third of web users have admitted to using the same password for a number of different websites, says Sophos.

According to the security firm, just 19 percent never use the same password twice. Sophos added that three years ago, 41 percent of web users said they used the same password, indicating that just 8 percent of web users have realized the importance of strong, unique passwords.

"It's worrying that in three years very few computer users seem to have woken up to the risks of using weak passwords and the same ones for every site they visit," said Graham Cluley, senior technology consultant at Sophos.

"With social networking and other internet accounts now even more popular, there's plenty on offer for hackers and by using the same password to access Facebook, Amazon and your online bank account, you're making it much easier for them. Once one password has been compromised, it's only a matter of time before the fraudsters will be able to gain access to your other accounts and steal information for financial gain."

PEOPLE WHO READ THIS ALSO READ:

- A Way to Sniff Keystrokes From Thin Air
- Why You Need a Password Manager
  1,248 PEOPLE VIEWED THIS
- Comcast's VoIP Makes It a Top 3 Telco
- Top Password Tips
- Could You be Hacked Like Twitter?
- Twitter Hacked, Secrets to be Revealed?

Recommendations by loomia

Threat: Weak Passwords

- Fact: Passwords are inherently weak.
- If 90 day interval, 3% use "SeasonYear"
- Steps to thwart this attack vector:
  - Establish strong password standards
  - Equip employees with password wallet technology
  - Supplement with two-factor
  - Train employees
  - Test passwords with password cracking
  - Credential capture, MINIMIZE the use of Admin Accounts
  - 80% of attacks hijack admin passwords
  - Admin account logging, alerts and monitoring – 1 minute

Strong Passwords are:

- ✓ Lengthy (at least 8, more is better, consider 14+)
- ✓ Complex (mix upper/lower/numbers, characters)
- ✓ Known only by authorized user
- ✓ **Unique per Use**
- ✓ Unique from any personal attributes
- ✓ Unique from any personal passwords

Use Routine Character Substitution for Websites

Choose a Consistent and Secret Technique you will use to change easily remembered passwords.

Example: Prefix is '8720' (address) + A through M becomes 3

Great for Websites:

Amazon = 8720333zon
Costco = 87203ost3o
Facebook = 872033333oo3

Keep your Routine Character Substitution pattern a Secret and change once a year!

Use a Password Wallet for Important Passwords

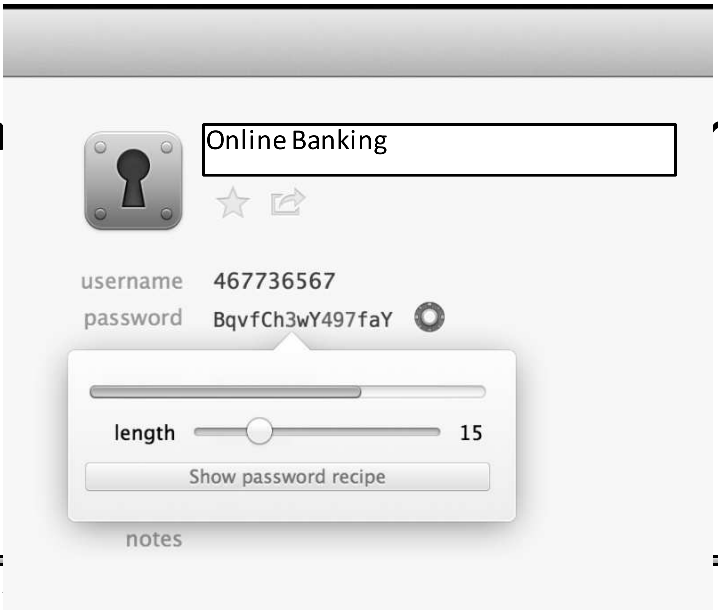
We do not recommend Routine Character Substitution for your most important passwords.

- Work
- Online Banking
- Investments and Insurance Sites

- Long Complex pws are the very best: J29NL7bnuzUv6Tc or Pacino15myFAVORITE!

- *Password wallets allow smart people to securely store all of your passwords, credit cards, software licenses and more.

In rd

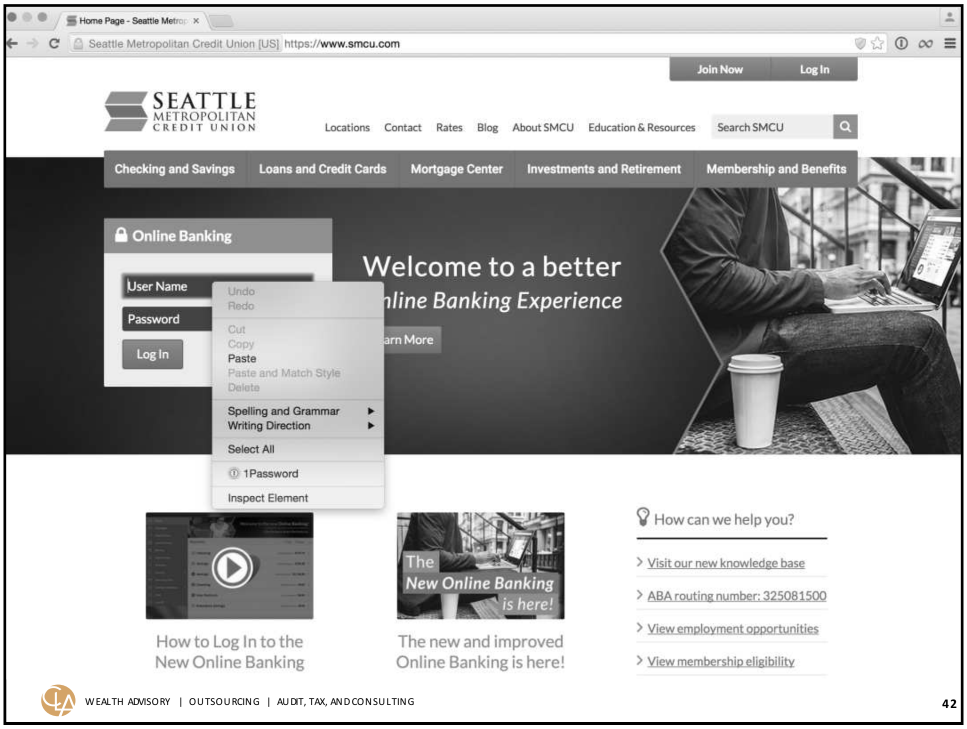


Online Banking

username 467736567

password BqvfCh3wY497faY

length 15



Welcome to a better
nline Banking Experience

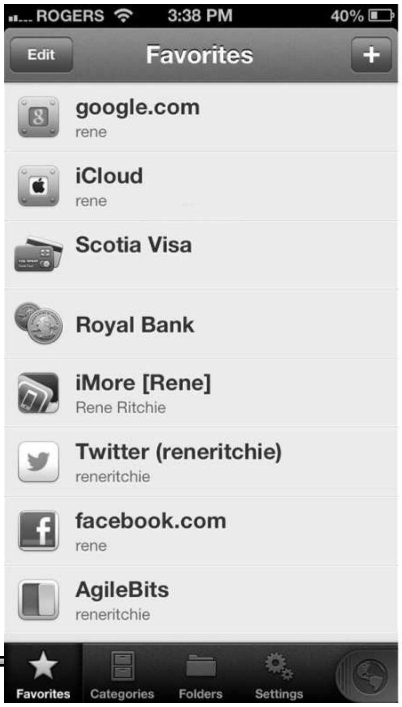
The New Online Banking is here!

How to Log In to the New Online Banking

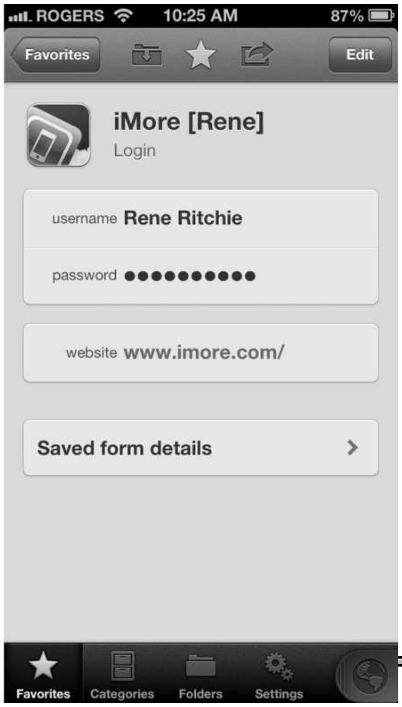
The new and improved Online Banking is here!

How can we help you?

- Visit our new knowledge base
- ABA routing number: 325081500
- View employment opportunities
- View membership eligibility



google.com	rene
iCloud	rene
Scotia Visa	
Royal Bank	
iMore [Rene]	Rene Ritchie
Twitter (reneritchie)	reneritchie
facebook.com	rene
AgileBits	reneritchie



iMore [Rene]
Login

username Rene Ritchie

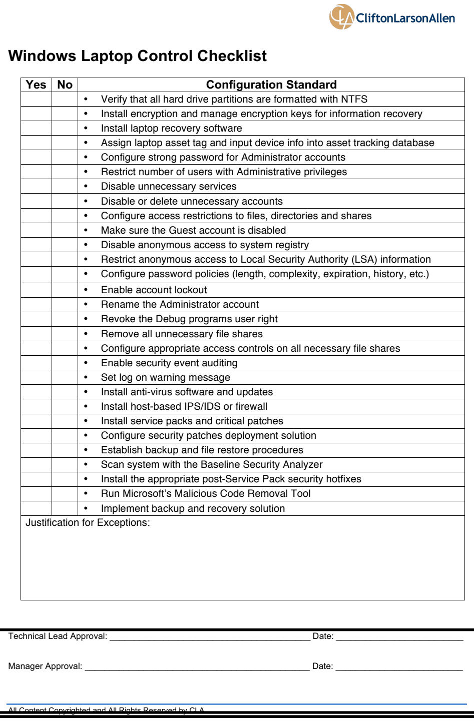
password ●●●●●●●●●●

website www.imore.com/

Saved form details

Threat: Weak Configuration

- Windows, despite considerable effort, remains vulnerable to many exploits.
- Attackers WILL locate the weakest link. We routinely find 90% of systems well configured.
- Steps to thwart this attack vector:
  - Regular credentialed vulnerability scanning
  - Remediate vulnerabilities
    - ◊ Patching, configuration, end-of-life
  - Minimal risk acceptance, actively avoid risk acceptance
  - Establish and enforce expectations (standards) for ALL SYSTEMS, including vendors.
  - Document and revisit exceptions.



CliftonLarsonAllen

Windows Laptop Control Checklist

Yes	No	Configuration Standard
		• Verify that all hard drive partitions are formatted with NTFS
		• Install encryption and manage encryption keys for information recovery
		• Install laptop recovery software
		• Assign laptop asset tag and input device info into asset tracking database
		• Configure strong password for Administrator accounts
		• Restrict number of users with Administrative privileges
		• Disable unnecessary services
		• Disable or delete unnecessary accounts
		• Configure access restrictions to files, directories and shares
		• Make sure the Guest account is disabled
		• Disable anonymous access to system registry
		• Restrict anonymous access to Local Security Authority (LSA) information
		• Configure password policies (length, complexity, expiration, history, etc.)
		• Enable account lockout
		• Rename the Administrator account
		• Revoke the Debug programs user right
		• Remove all unnecessary file shares
		• Configure appropriate access controls on all necessary file shares
		• Enable security event auditing
		• Set log on warning message
		• Install anti-virus software and updates
		• Install host-based IPS/IDS or firewall
		• Install service packs and critical patches
		• Configure security patches deployment solution
		• Establish backup and file restore procedures
		• Scan system with the Baseline Security Analyzer
		• Install the appropriate post-Service Pack security hotfixes
		• Run Microsoft's Malicious Code Removal Tool
		• Implement backup and recovery solution

Justification for Exceptions:

Technical Lead Approval: ______________________________ Date: ________________

Manager Approval: ______________________________ Date: ________________

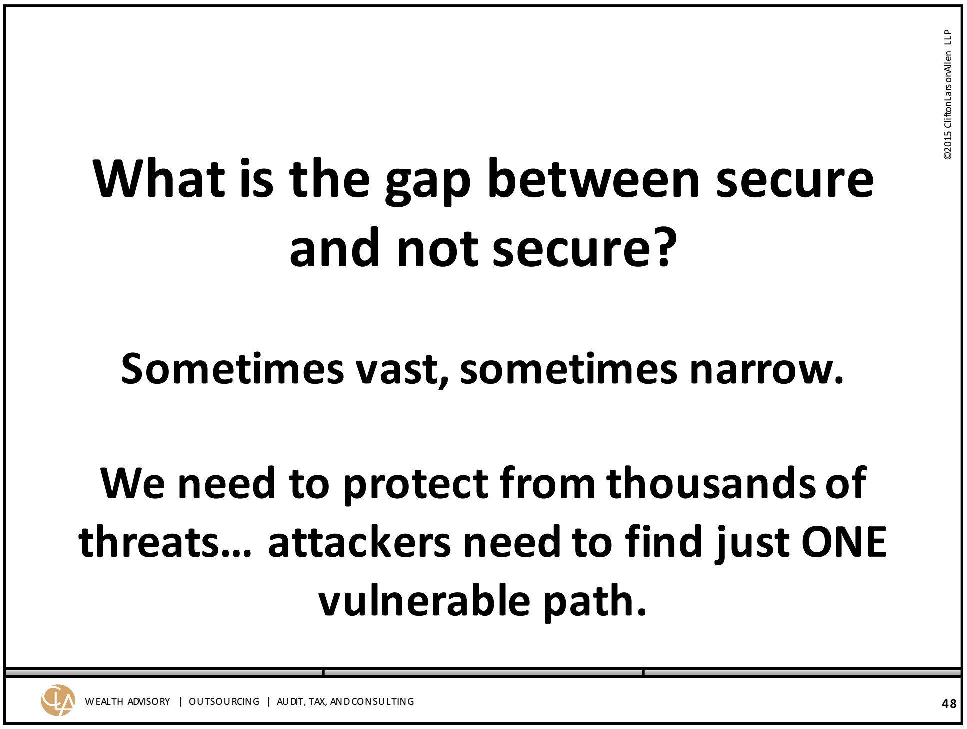
All Content Copyrighted and All Rights Reserved by CLA

Threat: Unknown systems and software

- If an attacker can engage unknown hardware or unknown software into the environment… advantage attacker!
  - Rogue wireless
  - Key loggers
  - Modified executables
- Steps to thwart this attack vector:
  - Hardware Pre-authorization
  - Control Local/Domain Admin
  - Detection of unknown hardware and software

Security Awareness Training

- Security Training is an important part of any security program but is largely ineffective if not supported by consequences.
- Password Training
- SE Avoidance
- Safe email and web surfing practices.



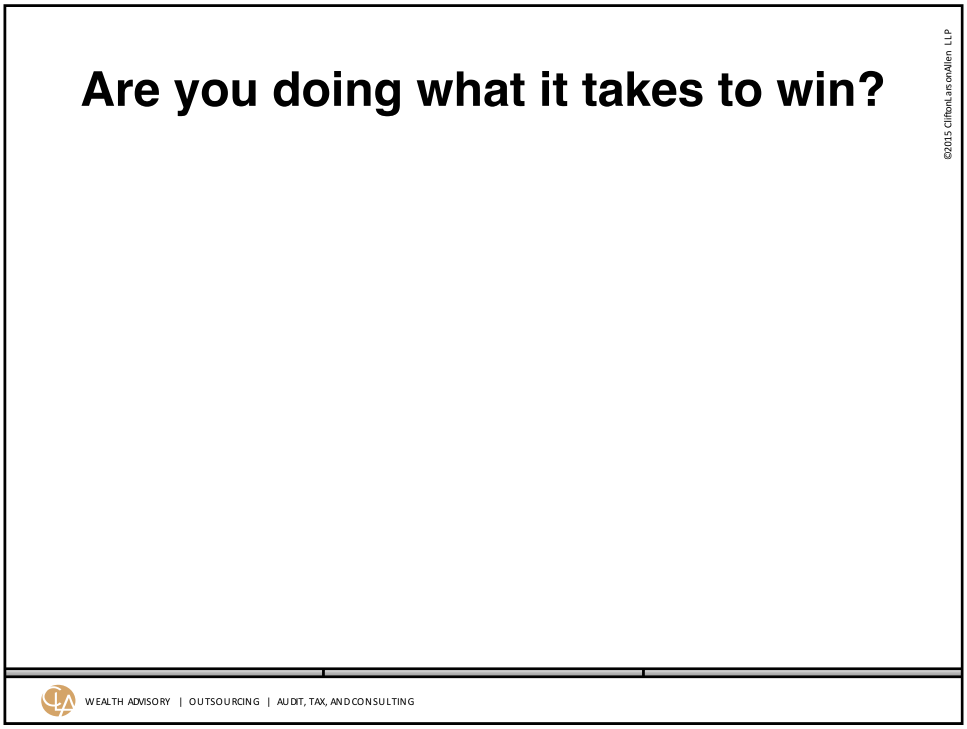
What is the gap between secure and not secure?

Sometimes vast, sometimes narrow.

We need to protect from thousands of threats… attackers need to find just ONE vulnerable path.

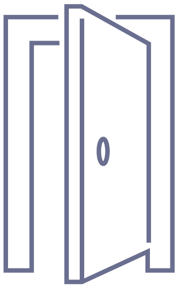
WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

48



Are you doing what it takes to win?

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING



Tom Schauer, Principal
CliftonLarsonAllen
Information Security Services Group
tom.schauer@CLAconnect.com
253-468-9750

CLAconnect.com

CliftonLarsonAllen

linkedin.com/company/
cliftonlarsonallen

facebook.com/
cliftonlarsonallen

twitter.com/CLAconnect