Information Security Risk Assessments
What, How and Why

1

Disclaimer

The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.

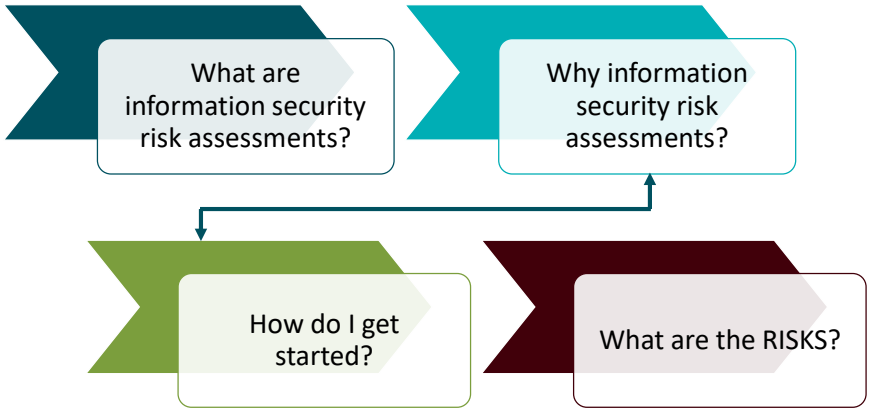
No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.

"Information Security Risk Assessments What, How and Why" discussed in this presentation is the current version with effective date of March 20, 2019.

The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.

2

Agenda



3

WHAT ARE INFORMATION SECURITY RISK ASSESSMENTS?

4

What is Information Security?

- **Information Security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption.**

5

What is Information Security?

- **Confidentiality – protecting information from being viewed by unauthorized users**
- **Integrity – information most remain accurate and complete and cannot be change by unauthorized users.**
- **Availability – information needs to be available when needed by those authorized to view the information.**

6

What is Information Security?

- **Information Security is not:**
  - **FFIEC Cybersecurity Assessment Tool**
  - **Equipment**
  - **Stagnant**
  - **Compliance**

7

Information Security Risk Assessment

- **An information security risk assessment is….**
  - **An on-going process of discovering, correcting and preventing security problems**

- WhiteHat Security

8

Information Security Risk Assessment

- **A risk assessment is not:**
  - **Vulnerability Scans**
  - **Questionnaire**
  - **Audit**
  - **FFIEC CyberSecurity Self-Assessment Tool**

9

Information Security Risk Assessment

- **Risk Assessment must include the following four steps:**
  - **Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;**
  - **Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the member information;**
  - **Assessing the sufficiency of the policies, procedures, member information systems, and other arrangements in place to control the identified risks; and**
  - **Applying each of the foregoing steps in connection with the disposal of information.**

06-CU07 Letter to Credit Union IT Security Compliance Guide

10

Information Security Risk Assessment

FFIEC

- To effectively identify, assess, monitor, and manage the risks associated with IT operations, management should have a comprehensive understanding of the institution's operations universe
- Management should analyze the survey of the IT operations environment and the inventory of technology resources to identify threats and vulnerabilities to IT operations. The assessment process should identify:
- Internal and external risks;
- Risks associated with individual platforms, systems, or processes as well as those of a systemic nature; and
- The quality and quantity of controls.

11

WHY INFORMATION SECURITY RISK ASSESSMENTS?

12

Why Information Security Risk Assessments?

NCUA 748 Part A III

- **Assess Risk. Each credit union should:**
  1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;
  2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and
  3. Assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.
- **Manage and Control Risk. Each credit union should:**
  1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities.

vizo financial

13

Information Security Risk Assessment

- **The risk assessment drives the rest of the information security program.**
- **Responsibility rests at the board level**
- **Find gaps and close those gaps**
- **Annual Process**

vizo financial

14

Why Information Security Risk Assessments?

- To protect our member's…..
  - NPI
    - (Non-public Personal Information)
  - PII
    - (Personally Identifiable Information)
- Sound familiar?
  - GLBA
    - Gramm-Leach-Bliley Act

15

HOW DO I GET STARTED WITH INFORMATION SECURITY RISK ASSESSMENTS?

CONNECT WITH US

16

How Do I Get Started?

- ISRAs are to be used in the following way.
  - Identify Assets.
  - Identify FORESEEABLE internal or external threats.
  - Identify if a vulnerability exists that could turn the threat into a RISK.
  - Drive decision making process to mitigate, accept or transfer the risk.

17

How Do I Get Started?

- Start by identifying assets
  - Hardware
    - PC, Servers, Printers, Switches, Firewalls, Smartphones, Laptops, Tablets, etc.
  - Software
    - Applications, programs, etc.
  - Websites
  - Data
    - Member information (PII/NPI)
    - Contracts

18

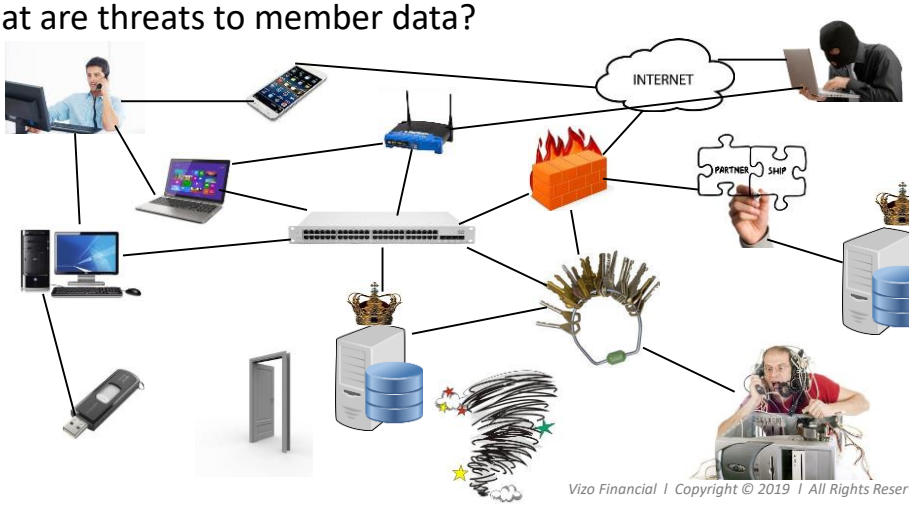
How do I get started?

- **What are the "Crown Jewel" assets?**
  - **Databases**
  - **Server rooms**
  - **Filing cabinets**
  - **Cloud providers**
  - **Member data…..anywhere that your members data exists**
  - **Last, but certainly not least…..Your employees!**

19

Proceed with Identifying Threats

- What are threats to member data?



20

Final Steps

- Determine if your assets are vulnerable to the threats
- Calculate risk rating
  - Inherent risk = (probability) x (impact)
- Evaluate if current controls mitigate risks
- Calculate residual risk rating with controls
  - Residual risk = (probability) x (impact) - controls
- Determine if residual risk is acceptable or if additional controls/mitigations are needed

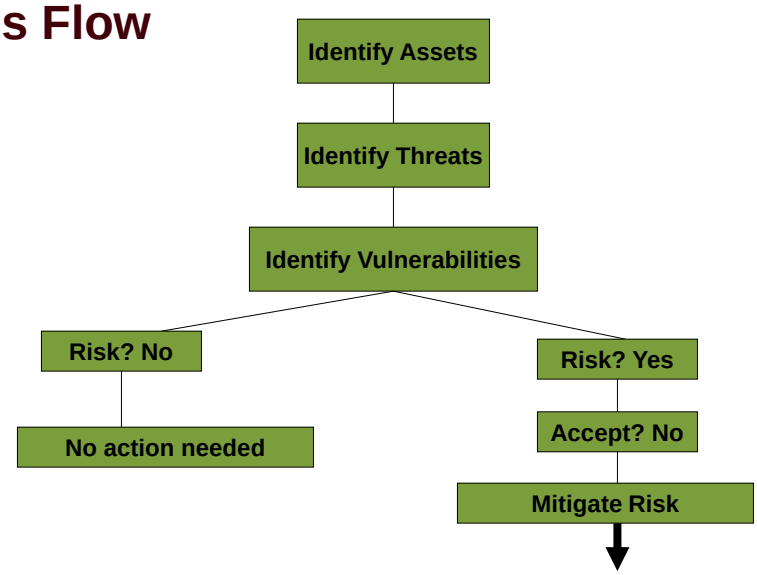
21

Final Steps

- How to handle gaps?
  - Remediate
  - Mitigate
  - Transference
  - Risk Acceptance
  - Risk Avoidance

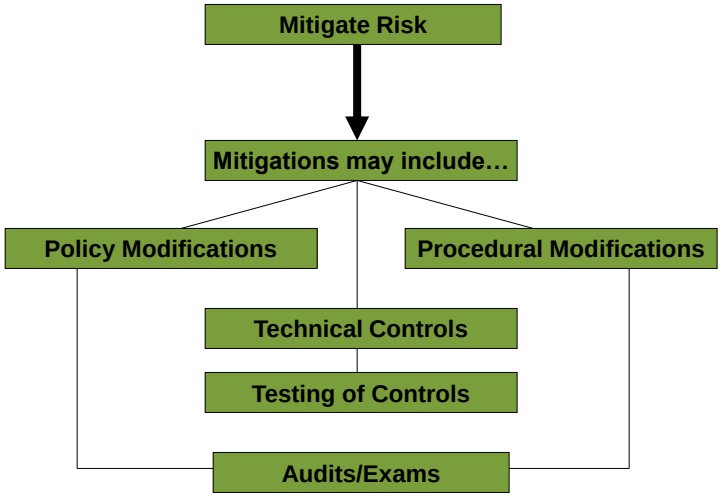
22

Process Flow



23

Process Flow



24

What happens…….

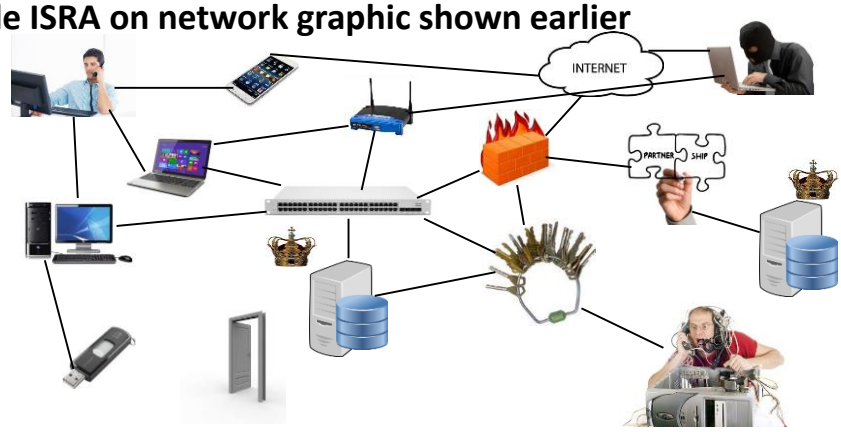
- If we don't do ISRAs
  - CIA/R
  - We might fail to provide continued CIA to our members
    - Confidentiality
    - Integrity
    - Availability
  - Our "R" could be tarnished..
    - Reputation

In Review So Far….

- We have discussed -
  - Why we need to do ISRAs
  - What the NCUA says about ISRAs
  - What the FFIEC says about ISRAs
  - How ISRAs help to shape Security Policies and Programs
  - How ISRAs lead to mitigations/controls
  - Some potential and actual consequences of not doing proper ISRAs

Basic Steps and Examples

- Sample ISRA on network graphic shown earlier



27

Basic Steps and Examples

- Gather Team for Brainstorming, Q&A Session
- Gather information about assets
  - Assets could be software, hardware, servers, databases, physical locations, lets not forget employees, etc.
  - Asset information could include access levels, network diagrams, current controls, version numbers, etc.
- Determine potential threats, vulnerabilities, risks

28

Basic Steps and Examples

- **Determine "Risk Rating" (Probability x Impact)**

	Impact	high	med-high	medium	med-low	low			
Probability		**5**	**4**	**3**	**2**	**1**		**Risk**	
high	**5**	25	20	15	10	5			**high**
med-high	**4**	20	16	12	8	4			**med-high**
medium	**3**	15	12	9	6	3			**medium**
med-low	**2**	10	8	6	4	2			**med-low**
low	**1**	5	4	3	2	1			**low**

29

Basic Steps and Examples

- **Determine definition around the rating**

Probability	
5	Happens all the time from most sources
4	Happens on a weekly basis from many sources
3	May happen once or twice a month from many sources
2	May happen once or twice a year from a few sources
1	Has never happened
(Note: The probability statements above represent the likelihood of a successful exploit occurring at **ANY** financial institution within the US financial system)	
Impact	
5	Devastating - all members severely affected, financial bankruptcy, irreparable reputation damage, uncontrolled information in the press
4	Severe - most members adversely affected, financial restructuring, heavy but recoverable reputation damage, voluntary press release
3	Moderate - many members affected, reportable financial losses, reputation adversely affected, voluntary communication to all members
2	Slight - few members affected, negligible financial loss, slight reputation damage, communication to affected members
1	Negligible - members, financials and reputation unaffected
(Note: The impact statements above represent potential adverse results to **YOUR** financial institution, stemming from a successful exploit)	

30

Basic Steps and Examples

- **Some sample questions and answers -**

  - **Do employees receive security awareness training?**
    - **Several years ago we watched a video.**
  - **Is there a list of all devices and software?**
    - **Our IT vendor takes care of that.**

31

Basic Steps and Examples

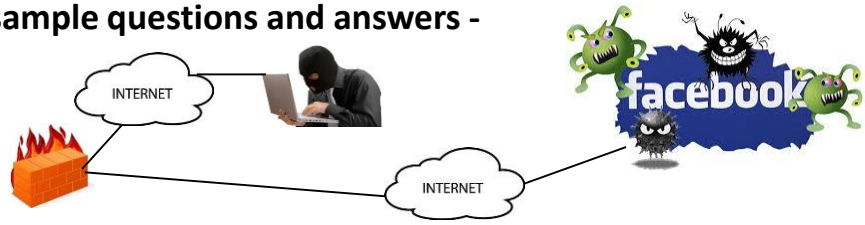
- **Some sample questions and answers -**

  - **Are software/OS patches and antivirus updates installed regularly? –**
    - **Isn't that automatic with Microsoft?**
  - **Are restores of backed up data tested regularly?**
    - **Last year our IT guy restored a Justin Bieber MP3 that I deleted.**

32

Basic Steps and Examples

- **Some sample questions and answers -**

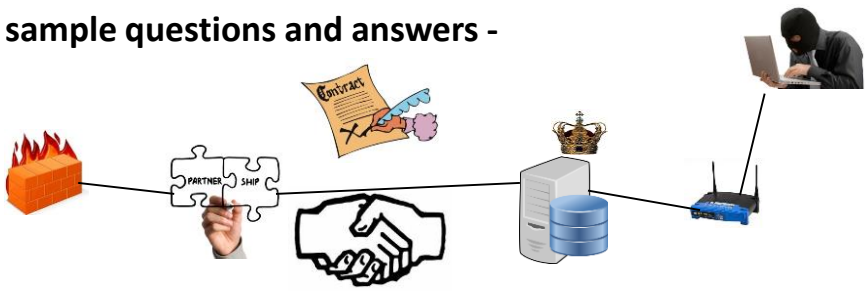


  - **Is your firewall policy reviewed for proper rules?**
    - **Policy, rules? Don't firewalls just know to stop bad guys?**
  - **Do you have any kind of web filter in place?**
    - **No, but we tell employees to only use Facebook during lunch.**

33

Basic Steps and Examples

- **Some sample questions and answers -**



  - **Do you monitor who connects in from your partner VPN?**
    - **Of course not, we have a contract, we trust them?**
  - **Is their network secure where your data is stored?**
    - **I'm sure it must be…..like I said, we have a contract.**

34

Available ISRA Methods

- OCTAVE (CERT)
- NIST 800-30 and 800-53
- ISO/IEC 27005
- ISACA Cobit and Risk IT
- CRAMM
- IRAM (ISF)
- Many commercially available vendors

35

Contact Information

John Cuneo
Information Security Director
jcuneo@vfccu.com
Toll-Free (800) 622-7494
Phone (717) 985-3300 ext. 1202
Vizo Financial Corporate Credit Union

36