LEVEL UP

Gene Fredriksen

Exam Futures: If You Stay Ready, You Don't Have to Get Ready

1

Disclaimer

A Few Things First

This presentation is for information only.
Evaluate risks before acting based on ideas from this presentation.

This presentation contains opinions of the presenters.
Opinions may not reflect the opinions of Tandem.

This presentation is proprietary.
Unauthorized release of this information is prohibited.

2

Gene Fredriksen

Executive Director – NCU-ISAO

3

LEVEL UP

THANKS FOR JOINING!

2023 Exam Priorities Getting and Staying Ready

Gene Fredriksen

CISM CRISC

National Credit Union ISAO

Gene.Fredriksen@ncuisao.org

609-712-0985

4

Agenda

The Plan for Today

- The Elephant in the Room
- The Priorities
- Risk Program Components
- Bringing it on Line
- Baking It In

5

NCUA 2023 Supervisory Priorities

The Elephant in the Room: Risk Management

- **Interest Rate Risk**
- **Liquidity Risk**
- **Credit Risk**
- **Fraud Risk- Prevention & Detection**
- **Information Security Risk (Cybersecurity)**
- **Consumer Financial Protection**

6

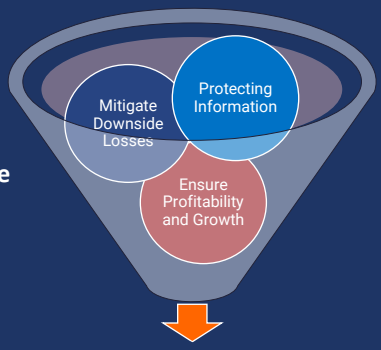
Overview – Risk Management vs. Identification

- **Given:**
  - Significant cyber-attacks are occurring more frequently
  - No company or organization is immune
  - The effects of a breach can significantly impact the profitability of a company long-term resulting in risks to investors
- **Therefore:**
  - Credit Unions must report significant breaches
  - The Board should include formal actions to monitor, assess, and govern Cyber security based on the company's risk profile
- **Barriers:**
  - Uncertainty regarding what is expected or required
  - FFIEC guidance and Cyber security legislation is constantly changing
  - Audit Committees traditionally focus on financial risk so significant cyber security expertise may not be available to the Board.

7

What is the CU's Role in Mitigating Cyber Risk? Oversight

- **Oversight means providing:**
  - management with guidance
  - approve information security plans, policies and programs
  - review reports on the effectiveness of the information security program
- **Provide management with expectations and requirements and hold management accountable for**
  - Central oversight and coordination
  - Assignment of responsibility
  - Risk assessment and measurement
  - Monitoring and testing,
  - Reporting
  - Acceptable residual risk



8

Start with a Risk Assessment
7 Crucial Questions to Ask

- What Are Our Most Important Assets? ...
- What Risks Do You See? ...
- What Strategies Do You Suggest to Mitigate the Risks? ...
- What Are the Strengths of Our Current Security System? ...
- What Overall Solutions Are Necessary? ...
- What Other Products Might We Need?

9

Risk Assessment: Get Started

Functional Area	Importance 1 (low) to 10 (high)	Risk Level 1 (low) to 5 (high)	Risk Score	Risk Category	Control	Mitigated Value	Mitigated Risk Score	Mitigated Risk Category
Access Control								
Formal standards for network access and passwords	8	3	24	Average Risk		20	4	Low Risk
User access to server(s) and files properly controlled	8	3	24	Average Risk		20	4	Low Risk
Review of network access & error logs	8	3	24	Average Risk		18	6	Low Risk
User access based on 'least privilege' consistent with job function	8	3	24	Average Risk		20	4	Low Risk
Default usernames are disabled and/or have complex passwords.	10	5	50	**High Risk**		35	15	Below Average Risk
Ensure user identity & that access is authorized	9	4	36	**Above Average Risk**		25	11	Below Average Risk
Use of utility programs capable of overriding application controls restricted	6	5	30	Average Risk		28	2	Low Risk
Restrictions placed on connection times to provide additional security	5	3	15	Below Average Risk		12	3	Low Risk

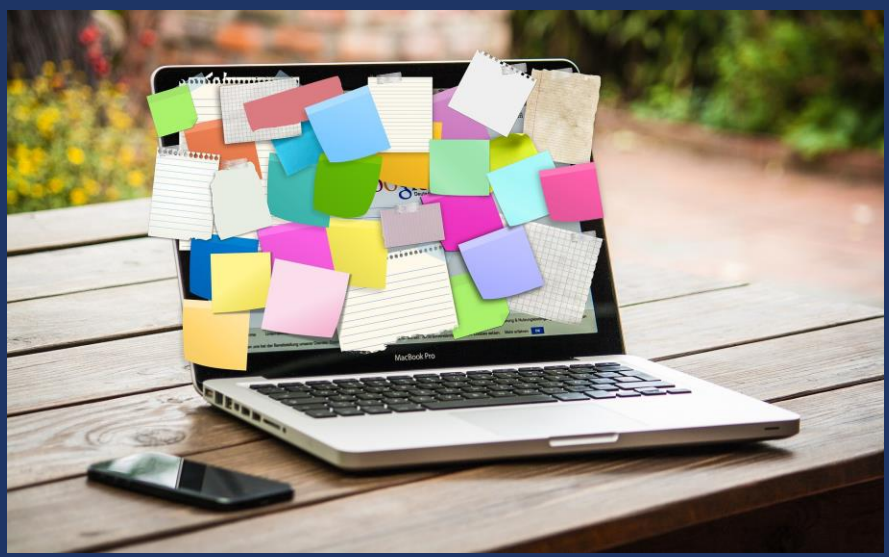
10

Risk Management Components

- Audit Management
- Identity Theft Prevention
- Policies
- Business Continuity Planning
- Incident Management
- Risk Assessment
- Compliance Management
- Internet Banking Security
- Vendor Management
- Cybersecurity
- Phishing

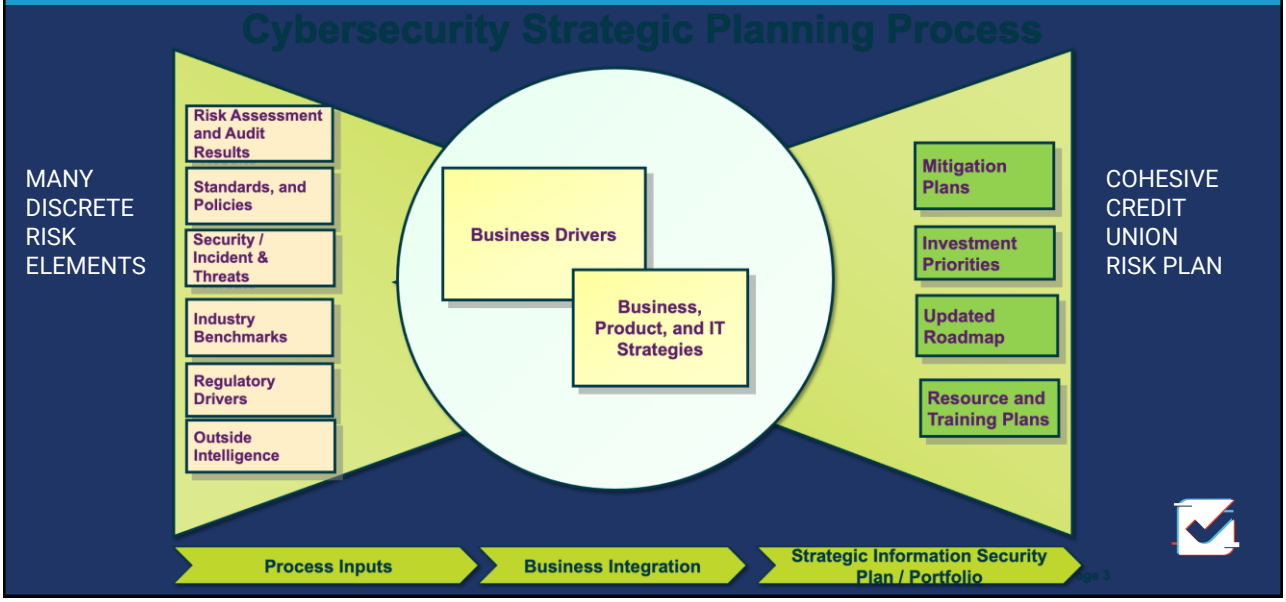
11

This is Not a Risk Management System



12

Sustainable Risk Mitigation Plan



13

Key Business Driver(s)

Standards, and Policies

- Standard guidance to streamline compliance activities (reduce project delays and achieve consistent operations)
- Standard guidance to avoid fines, sanctions, and adverse publicity
- One voice when responding to customer inquiries regarding security
- Regulatory focus changing to methodology.

Key Risk Mitigation Activities

- Support NCUA requirements including User Access Attestation
- Uniform Policies for CU aligned to FFIEC security framework
- Perform ongoing benchmarks with our peers
  - FFIEC Cyber Security Framework Review
- Education on cyber assessment methodology
  - Emerging NCUA Standard

14

Security Monitoring and Incident Response

Security / Incident Monitoring

Key Business Driver(s)

- Achieve compliance with required regulations
  - Avoid fines, sanctions, and adverse publicity related to noncompliance
- Maintain business operations during an incident or breach
  - Execute response plans to control business data losses in the event of a data breach
- Enhance business awareness to potential security incidents which may affect operations
- Support HR and Legal investigations

Key Risk Mitigation Activities

- Enhanced Security Analytics system
- Participate in regular incident response tabletop exercises – NCU-ISAO

15

Benchmarking

Industry Benchmarks

Benchmark Partners

- Suppliers
- Similar CUs through NCU-ISAO

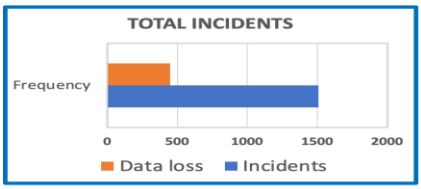
Key Risk Mitigation Activities

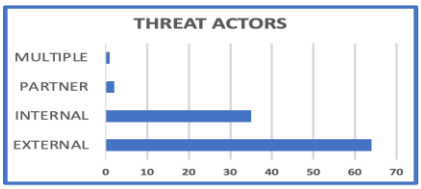
- Monitor regulatory changes NCUA / FFIEC
- Receive training on self assessment process
- Monitor emerging State Privacy Laws and requirements

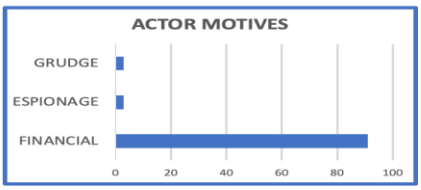
16

Industry Trends and Intelligence

Industry Benchmarks







Key risk Mitigation Activities

- Enhance our information sharing relationships InfraGard and NCU
- Increase participation in industry sharing forums with peers
- Training to increase the skill levels of CU Incident Response teams
- Increased frequency of security awareness messages to staff and management

17

Threat and Vulnerability Management

Outside Intelligence

Key Business Driver(s)

- We have valuable intellectual property, and others want to steal it

Key Risk Mitigation Activities

- Enhanced 24 X 7 systems monitoring and event correlation thru NCU-ISAO and Partners
- Enhanced Scanning to ensure patches are installed and function
- Discovery and reduction of files containing sensitive information
- Implementation of a document retention policy and mechanism to enforce

18

Member Input

Member Input

- Resilience – Service available when I need it most. (Disaster, Pandemic, etc..)
- Expectation that Products and Services will be Secure and Compliant
- Mobile Applications support
- Information Protection / Fraud Prevention Leadership

Key Risk Mitigation Activities

- Embed Security processes within IT functions
- Robust Access and Authorization functionality – 2FA
- Security Conference / WebCasts regarding Security Issues
- Training, Education

19

Business Drivers

Business Drivers

- Uptime
- Need for Agility
- Need for Stability
- Expectation that Products and Services will be Secure and Compliant
- Stability as post Covid activities occur

Key Risk Mitigation Activities

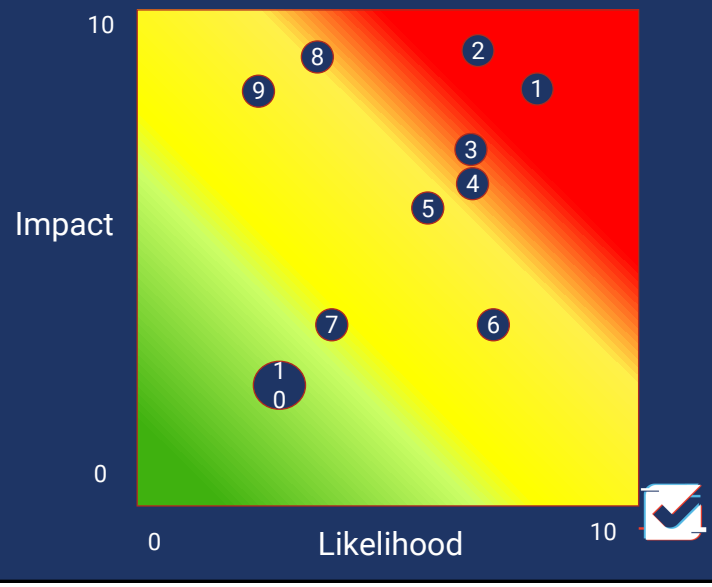
- Robust Access and Authorization functionality 2FA

20

Risk Rank Projects

- Ranking / Priority

#	Program	L	I
1	User Add change Delete Automation	**8**	**8**
2	Discovery and reduction of sensitive data files – e-shred	7	9
3	Network Scanner – Internal Processes	6	6
4	User Access Attestation	6	5
5	Incident Response Exercises / Training	5	5
6	Cyber Dashboard	7	4
7	General User Education - Cybersecurity	4	4
8	Password Manager Standardization	9	4
9	Compliance dashboard	4	8
10	Member Education / Blog	3	3



21

Annual "State of Cyber security" Report

- **Require an annual "State of Cyber security" report . The report should address:**
  - results of the risk assessment process
  - risk management and control decisions
  - service provider arrangements
  - results of security monitoring and testing
  - security breaches or violations and management's responses
  - recommendations for changes to the information security program
- **The review should consider:**
  - the results of management assessments and reviews
  - internal and external audit activity related to information security
  - third-party reviews of the information security program
  - other internal or external reviews designed to assess the adequacy of information security controls

State of Cyber security Report

22

Participate in Cyber Insurance Discussions

- Verify that the cyber insurance coverage is sufficient to address the potential cyber risks
- Ask management to provide the projected cost per record of data breach
- Understand the total potential impact of a major data breach

Cyber Insurance Review

23

Board Actions – Include in Minutes

Policy and Strategy Approvals

Cyber Priorities

Program Monitoring

Governance & Oversight

- **Review and Approve (Annually)**
  - Policies
  - Written Information security Plan
  - Cyber security Strategic Plan (includes funding and staffing)
- **Review Top 10 Cyber Risks (Annually)**
  - New and Emerging Threats
  - Regulatory Mandates
- **Board or Audit Committee Cyber security Updates**
  - Key Risk Indicators
  - Progress against Risk Mitigation Plans
  - Funding and Staffing
- **Cyber security Program Health**
  - External Audits and Assessments
  - Internal Audit
  - Regulatory Comments
  - Breach Reporting

24

Adequate Access to Consistent Cybersecurity/Risk Expertise is Important

- **FFIEC Expectations: Board includes risk and cyber expertise, just as they include seasoned financial and operational expertise**
- **Augment existing cyber skills with an advisors / partners possessing significant experience and expertise, providing:**
  - Expert review of company strategies, reports, and plans
  - Assistance in understanding Company's security strategy and current projects
  - Assistance in identifying key roadblocks (e.g., budget, political agendas, arrogance)

25

Summary

- **Cybersecurity will continue to pose a serious risk that Cus muxt actively actively measure and continuously monitor**
- **The FFIEC will continue to mandate additional governance and oversight responsibilities for Boards**
- **The onus is on the Board to take its strategic role seriously in providing oversight**
- **Identifying the person responsible for the overall cyber security program is the first step**
- **Cybersecurity is no longer simply another agenda item for IT; it is an agenda item for the Board as well**

26

NCU-ISAO Services Ncuisao.org

NCU-ISAO Security Awareness Intelligence Information Sharing

Enabling bi-directional information sharing of cyber threat indicators, incidents, observables, threat actors, tactics, techniques and procedures, exploit targets and campaigns.

Credit Union Cybersecurity Regulatory Intelligence

Providing information, intelligence and benchmarking information related to NCUA, FFIEC, PCI and other related guidance including the effective use of the self-assessment tools.

Credit Union Cyber Resilience Operational Guidance

Harmonizing leading practice focusing on people, process and technology - defining credit union-specific cybersecurity operational guidance, tools, templates and resources - aligning with the business mission.

NCU-ISAO Cyber Education
Supporting security education as an enterprise-wide effort through workforce education and daily situational awareness, while enabling collaboration with Annual Incident Response Exercises to learn and practice cyber skills through vetted, plausible scenarios.

Enhancing Credit Union Cyber Resilience Through Information Sharing, Intelligence, Operational Guidance, and Workforce Education

27