Risk Ranking your Credit Union

Jim Brahm, President/CEO,
Security Compliance Associates, Clearwater, FL

June 6th, 2017

Bios

Jim Brahm, Managing Director and CEO for Security Compliance Associates (SCA) which delivers security assessments, compliance and control reviews and other services

- 26 year career with FIS, Certegy, Equifax Card Services and Telecredit
- Most recent role at FIS was SVP and Chief Operating Officer for the Card Services Division, which include 4 large business units and over 1,000 associates

Topic

“While various layers of technology controls, from the firewall to the desktop, must be implemented to protect sensitive data, technology controls alone are not effective. This session discusses the implementation of simple risk Assessment processes to identify Threat vectors and creating a sustainable process to assess risk and know where you stand as an ongoing process, to help create a robust defense against data loss.”

Agenda

- The Threat Environment
- Laws & Regulations
- Risk Assessment Process
- Lines of Defense
- The Future
- Q & A

The Threat Environment

- Hacker breaches security at Pentagon Federal Credit Union
- Big Banks Hit With Denial of Service Attacks
- Ransomware – WannaCRY?
- **EternalRocks Worm Spreads Using 7 Leaked NSA Exploits**
- As Mobile Devices Catch On with Businesses, Data Breach Risks Grow
- Intelligent Adversaries
- Rush of new technologies without due care
- Complacency and Rationalization
- Attack on Members Environment
- Response to Financial specific malware

Laws & Regulations

- Gramm-Leach-Bliley Act
  - Program designed to protect the confidentiality, security, and integrity of customer information, consumer information, and customer information systems
  - Objectives are to:
    - Ensure the security and confidentiality of customer information
    - Protect against any anticipated threats or hazards to the security or integrity of such information
    - Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer

Laws & Regulations

- Gramm-Leach-Bliley Act
  - Resulting Regulations
    - Privacy of Consumer Financial Information
    - Interagency Guidelines Establishing Information Security Standards
    - Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
    - NCUA Guidelines for Safeguarding Member Information
    - NCUA Guidelines for Response to Unauthorized Access to Member Information and Member Notice
    - Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Laws & Regulations

- Security Program Requirements
  - ***Perform risk assessments to identify <u>reasonably foreseeable</u> internal or external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems***
  - Consider appropriate access controls on customer information systems, including controls to authenticate and grant access only to authorized individuals and companies Consider appropriate access restrictions at locations containing customer information, such as buildings, computer facilities, and records storage facilities

Risk Assessment

Purpose

- The purpose of this risk assessment is to establish a baseline assessment of risk to protected information and the information systems that store and handle protected information. It will also identify threat actors, threat actions, controls (or lack of controls), likelihood of occurrence, resulting impacts to protected information if the controls are bypassed, and to recommend additional controls to mitigate the risk.

Risk Assessment

Scope

- This assessment applies to all protected information and the information systems that store or handle this information. All assets in all locations (software/applications, routers/firewalls, switches, workstations, laptops, servers, peripheral devices, and people) that are able to affect protected information have been taken into consideration. Administrative, physical, and technical controls have been identified at a high level to determine their existence, absence, and their general effectiveness, which has then been used in the measurement of likelihood and impact of a threat action.

Risk Assessment

Assumptions

- The extent of the information collected, tests or scans performed, and interviews with individual in various roles was primarily limited to the time spent on-site by the risk assessor. Extensive documentation is sought by the risk assessor and all that is provided by the institution was reviewed. Anything not provided or able to be found was assumed to not exist.

- While a risk assessment is not a formal controls review, general control effectiveness should be understood by the institution and risk assessor to effectively evaluate the risk. For controls that are not regularly tested and that have not been fully matured, a formal controls review is recommended to determine their true effectiveness and the lapses in expected coverage

Risk Assessment

Overview

- A risk assessment can be assessed using a qualitative and quantitative approach. Quantitative calculations employ a set of methods, principles, or rules for assessing risk based on the use of numerical values. Qualitative calculations employ a set of methods, principles, or rules for assessing risk based on nonnumeric categories or levels (e.g., low, medium, and high).

- Risk analysis is a methodology used to identify the threats, classify assets, and rate their vulnerabilities so that effective security controls can be implemented.

Risk Assessment

- Identify relevant threat actors and their actions
- Identify the protected assets
- Identify the asset attribute that the threat actions will affect
- Identify existing controls that are relevant to the actor, action, asset, and attribute
- Determine the likelihood that the identified threat action will occur
- Determine the impact of the threat action on the asset if the existing controls were to be bypassed
- Determine the information security risk as a combination of likelihood and impact
- Recommend additional controls that will reduce each risk

Risk Assessment

Methodology

- The methodology for assessing IT security risk (i.e. the preparation, conducting, and communication steps) is derived from the NIST Guide for Conducting Risk Assessments and follows the documented guidelines where feasible, commensurate to the size and complexity of the organization. Analysis approach is threat (the actors and actions) and asset oriented (the asset and attribute).

- The VERIS (Vocabulary for Event Recording and Incident Sharing) framework is also used for the common language and understanding of the analytic approach presented in the NIST Guide for Conducting Risk Assessments.

- The risk model contains the risk factors of threat actors, threat actions, assets, and the attribute affected. These four factors come from the VERIS framework to bring a vocabulary and understanding to these key factors. Whereas NIST defines several threat sub-categories, VERIS consolidates them into the threat actor. Threat events, as defined by NIST, are translated into threat actions by VERIS. For more specific understanding of the effect of the actor's actions, the asset and the asset's attribute (i.e. availability, confidentiality, and/or integrity) is identified to make implementing controls more effective and direct.

- Binary Risk Analysis tool is used to refine the risk level based on likelihood and impact to asset and organization, based on subjectivity of assessors knowledge of the environment.

Risk Assessment

Credit Union has the following responsibilities:

- Identify key assets and their criticality
- Make risk decisions (accept, avoid, mitigate, or transfer)
- Assign resources and actions to follow through with risk decisions
- Maintain and track existing risks and add new risks as they emerge

Risk Assessment

Likelihood[1]

Value	Description
High	Action is **highly likely** to occur.
Moderate	Action is **somewhat likely** to occur.
Low	Action is **unlikely** to occur.

Risk Assessment

Impact[2]

Value	Description
High	Expected to have **severe or catastrophic** adverse effects on protected information.
Moderate	Expected to have **serious** adverse effects on protected information.
Low	Expected to have **limited or negligible** adverse effects on protected information.

Risk Assessment

Risk[1]

Likelihood	**Impact**		
	Low	Moderate	High
High	Low	Moderate	High
Moderate	Low	Moderate	Moderate
Low	Low	Low	Low

[1] Based on the NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments definitions for Risk and Information Security Risk, Table I-2 Assessment Scale – Level of Risk

Threat Actors

External Threats	Internal Threats	Vendor Threats
Nature	Operations employee	Supplier
Activist	Ground team employee	Business associate
Competitor	End-User	Trusted outsider
Customer	Developer	
Ex-employee	System administrator	
Nation-state	Executive	
Hacker		

Threat Actions

Category	Actions
Malware	Viruses, Worms, Key loggers, Spyware, Backdoors, Trojan horses, Rootkits, Botnet, Ransomware, Watering hole
Hacking	Brute force, SQL injection, Cross site scripting, Cryptanalysis, Denial of service, Distributed denial of service
Social Engineering	Phishing (email, phone, mail), Blackmail, Threats, Scams, Eavesdropping
Misuse	Inappropriate use of email/network/web, Administrative abuse, Use policy violations, Use of non-approved assets
Physical	Theft, Tampering, Snooping, Sabotage, Local device access, Assault
Error	Omissions, Misconfigurations, Programming errors, Trips and spills, Malfunctions, Unauthorized use of copyright material, Disclosure of information
Environmental	Power failures, Electrical interference, Pipe leaks, Atmospheric conditions, Humidity, Heat wave, Ice storm, Tornado, Fire, Flood, Lightning

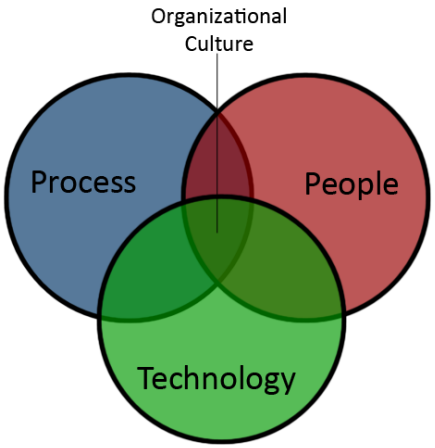
Binary Risk Analysis

Check all that apply:

- [x] The attack can be completed with common skills
- [x] The attack can be completed without significant resources
- [x] The asset is undefended
- [x] There are known weaknesses in the current defences
- [x] The vulnerability is always present in the asset
- [x] The attack can be performed w/o meeting pre-conditions
- [x] There will be consequences from internal sources
- [x] There will be consequences from external sources
- [x] The asset has or creates significant business value
- [x] The repair or replacement costs will be significant

Risk	Low
Likelihood	Low
Impact	Low

Control Types



People – Who we are

- Must be aware, diligent, adhere to policies and follow

Processes – What we do

- Repeatable steps (procedures) to accomplish business objectives
- Must be clear and unambiguous

Technology – What we use to improve what we do

- Must be configured properly and updated regularly

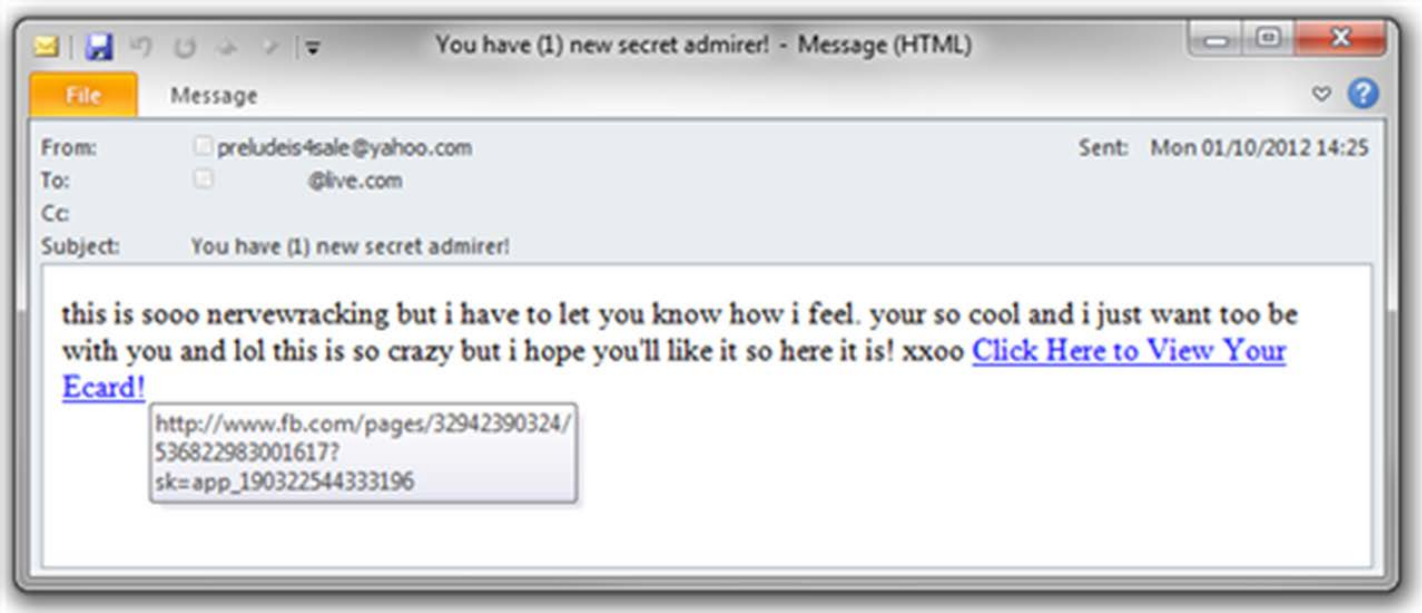
People Controls

Security Awareness Training

- New Hire Presentations
- Social Engineering Testing
- Ongoing Security and IT Risk Training
- Participation in October National Cyber Awareness Month including guest speakers, posters, and trinkets

People Controls

Phishing



People Controls

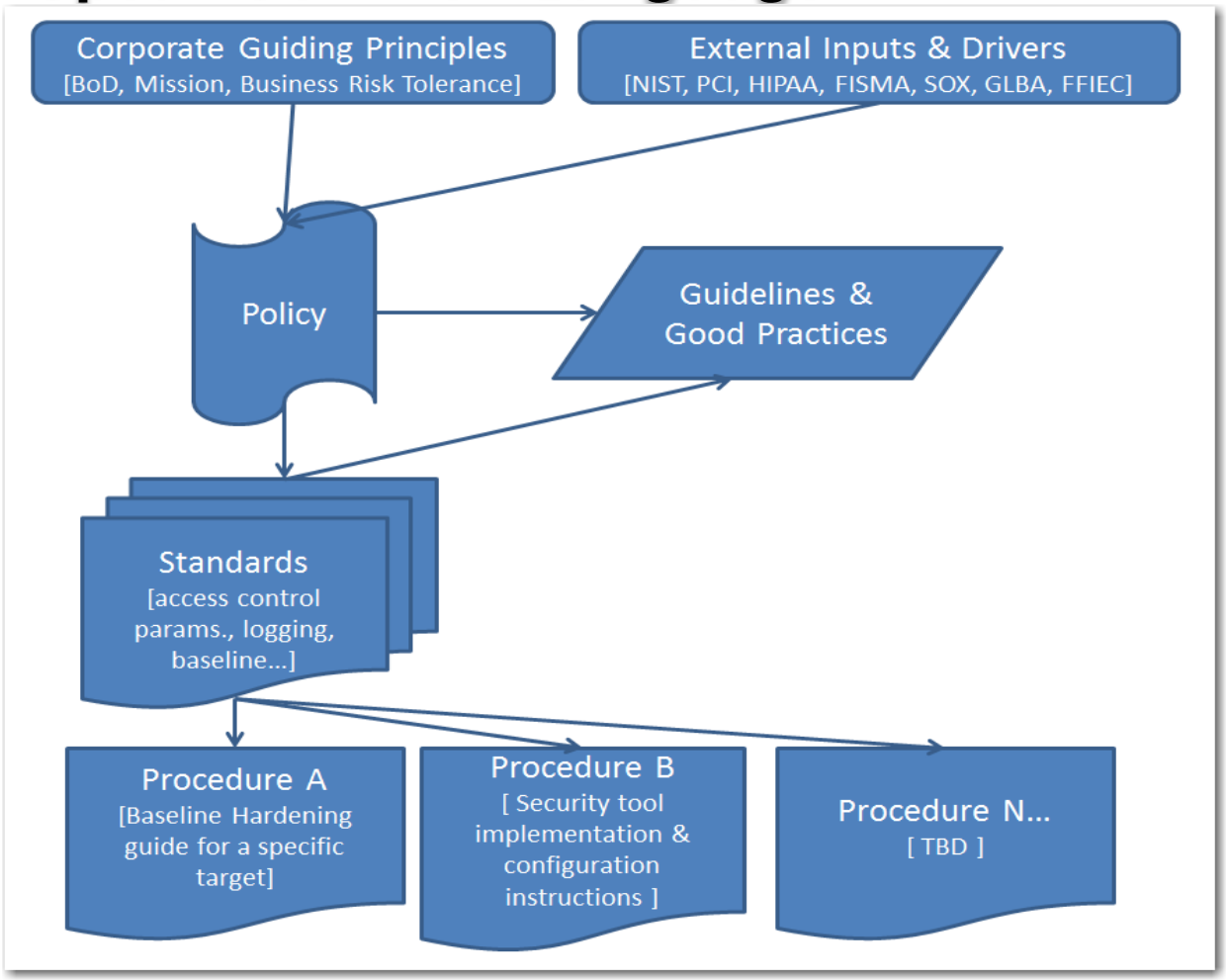
Google Terms of Service

Last modified: April 14, 2014

"When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content."

Process Controls

Speak Common Language



Laws
Regulations
Best Practices
Inflexible

Business Rules to apply Regulation to Practice
Rigid

Rules or mandatory action to support Policy
Somewhat Flexible

Operational steps to enforce policy
Flexible

Technology Controls

- Choose one or more Control Frameworks to meet compliance and security objectives
- Choose controls that map to the control framework(s) to meet compliance and security objectives
- Outsource what you don’t have expertise to perform in-house
- Test control effectiveness (internal and external)
- Don’t create excessive sophistication that hinders your ability to manage technology or monitor alerts

Future Recommended Direction

- Maintain Strong Information Security Program
- Focus on Existing and Emerging Threats
- Continuous Review/Test/Remediate
- Embrace Standards
- Proactively Adopt Standards
- Integrate Risk Ranking into ISP

Questions?

"The irony is, I'm doing time for crimes committed by the guy whose identity I stole."