Assigning Probability to Cybersecurity Risk

Jennifer Bayuk

Decision Framework Systems, Inc.

Historical Data Limitations

- In all of the successful cases of the application of probability theory to risk management, there has been a large quantity of suitable data collected over time wherein stable patterns are repeated.
- For example, credit risk decision is mostly based on analysis of historical data and the market risk decision is mostly based on analysis of potential future behavior.
- Risk-based models for technology operations that use aggregated data sets to forecast the future is today practiced mostly in academia and in large technology companies where automated processing is very homogeneous.
- Without having past data with which to develop models to predict the future, there is no way to agree on a base probability of a given event. As on expert put it, they are:*

  "computer gymnastics - subject to many of the same hurdles that stand in the way of conventional probability theory - the raw material of the model is the data of the past."

** Bernstein, Peter, Against the Gods, The Remarkable Story of Risk, John Wiley and Sons, 1996,*

Exemplar Enterprise Risk Management Framework Standards

- **COSO** – Committee of Sponsoring Organizations of the Treadway Commission, an independent private-sector association sponsored jointly by five major professional associations focused on financial statement integrity.* COSO's goal is to provide thoughtful leadership dealing with three interrelated subjects: Enterprise Risk Management (ERM), Internal Control, and Fraud Deterrence. COSO ERM Framework document is: ***Enterprise Risk Management: - Integrating with Strategy and Performance*, 2017.**
- **BIS** – The Bank of International Settlements (BIS) **Basel** Committee on Banking Supervision. A membership-based association of 60 central banks. The mission of BIS is to serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks. The BIS Operational Risk Management Framework is described in*: **Sound Practices for the Management and Supervision of Operational Risk* (BCBS96) 2003**, and subsequent enhancements to provide more detail on specific topics.

* The American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the Institute of Management Accountants [IMA]

NIST Warning:

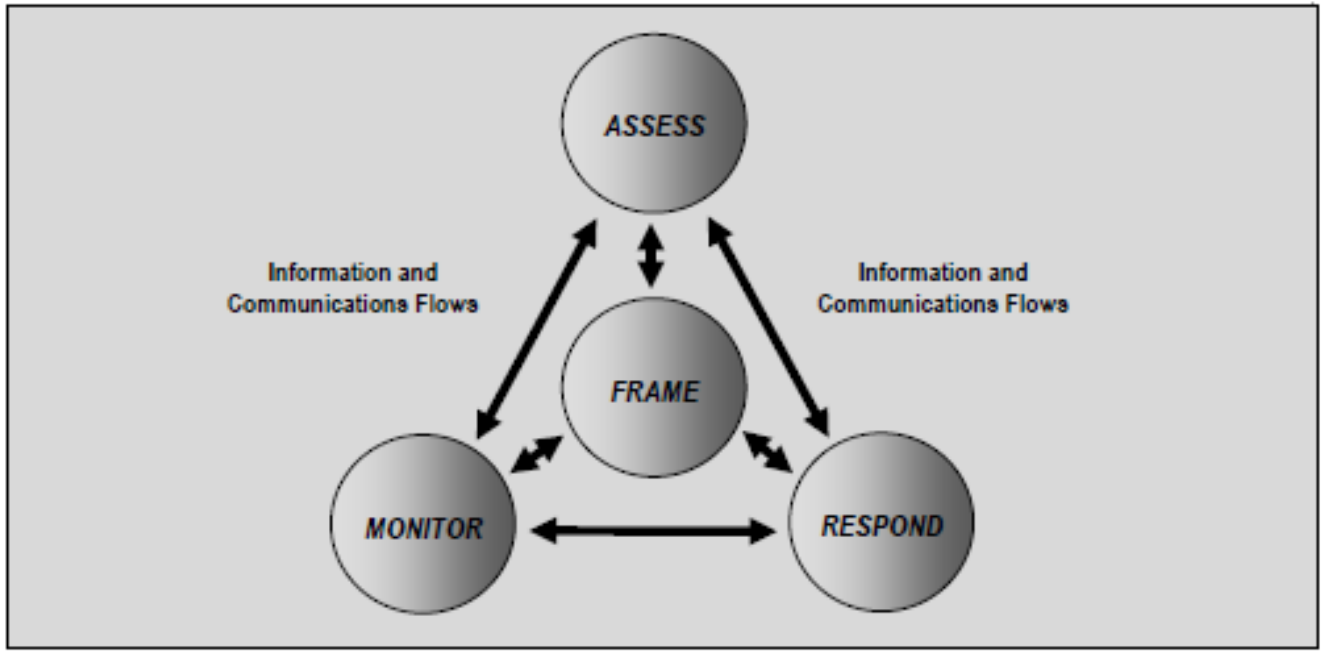


FIGURE 1: RISK ASSESSMENT WITHIN THE RISK MANAGEMENT PROCESS

The first component of risk management addresses how organizations *frame* risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a *risk management strategy* that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk management strategy establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.[14]

[1] *NIST SP800-30, Guide for Conducting Risk Assessments*

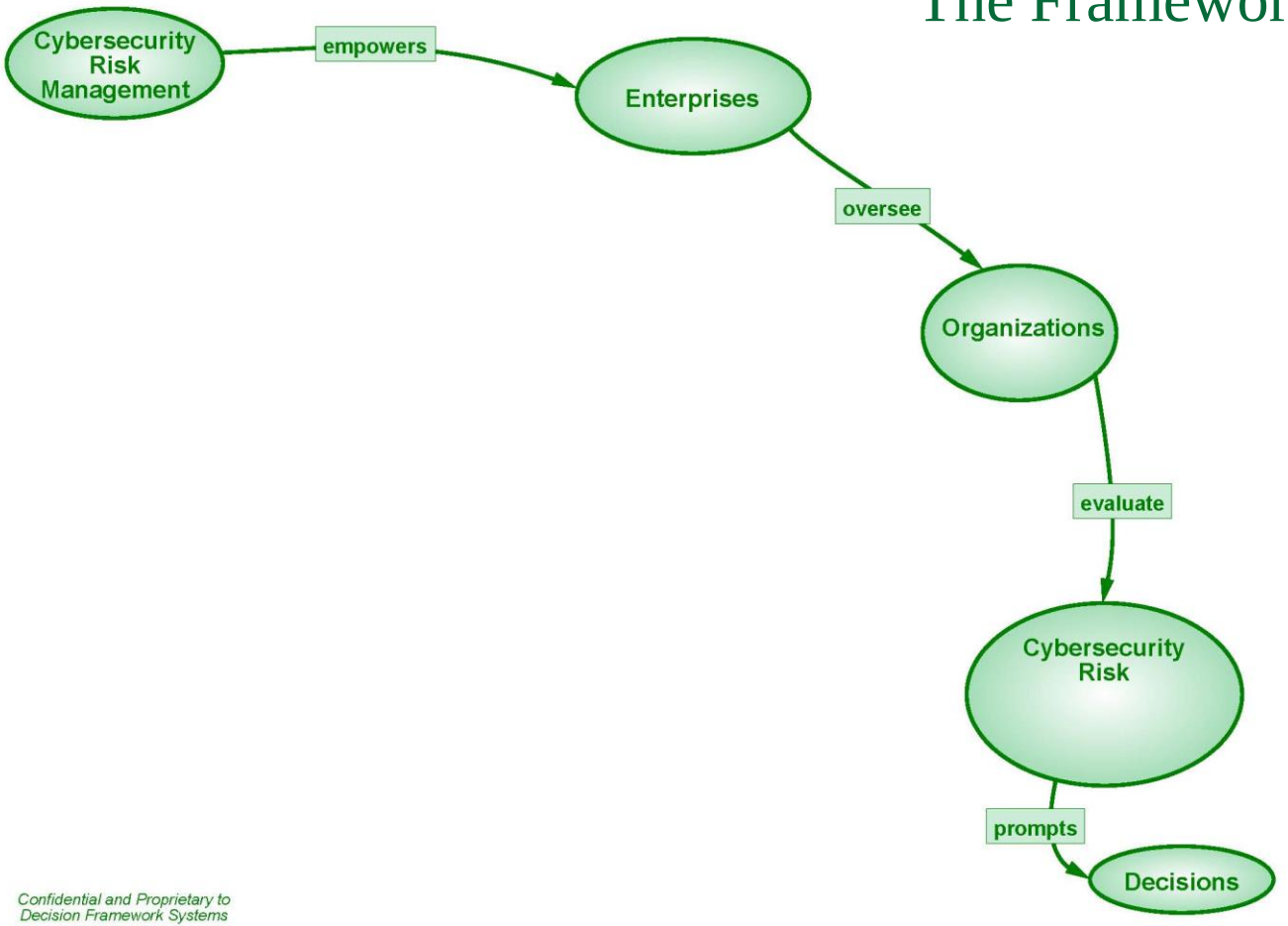
Framework Reflects COSO View of Risk Appetite and Tolerance

- ***Risk appetite*** is management's qualitative statement on risk tolerance, for example:

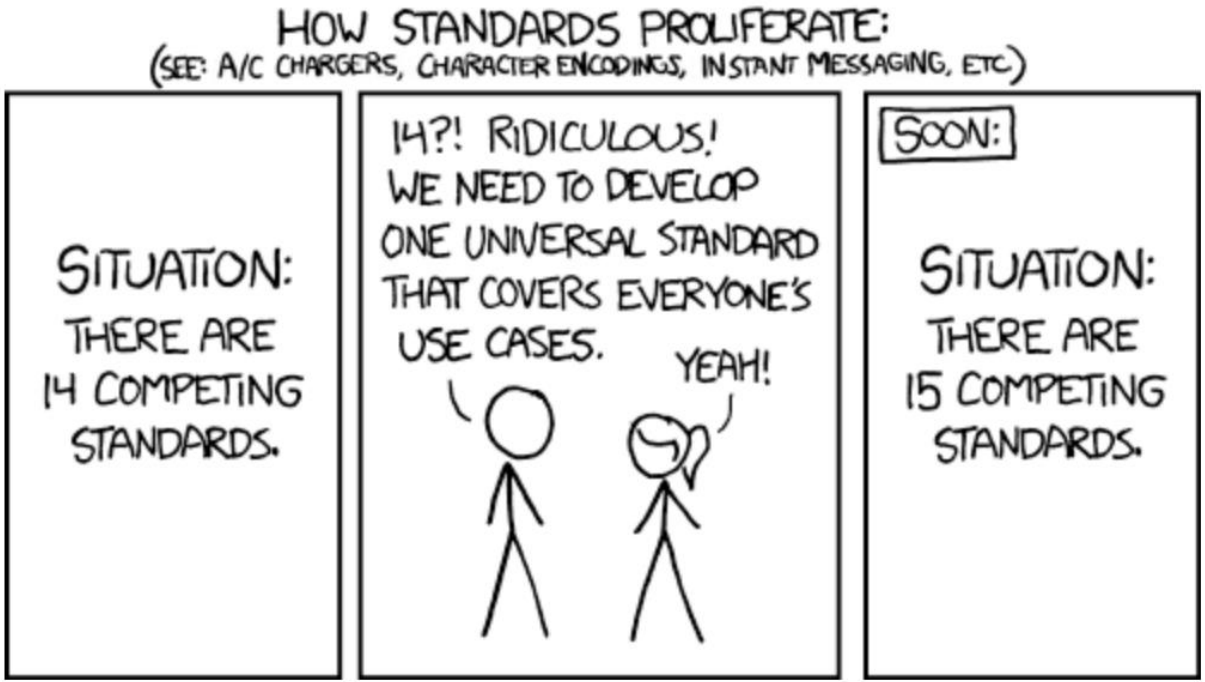
  Cybersecurity is a major concern. The firm has no tolerance for known vulnerabilities in its systems, no tolerance for data breaches, and low tolerance for unknown vulnerabilities.

- ***Risk tolerance*** refers to the range of degraded performance that management deems acceptable as a demonstration that risk appetite is observed.
- Risk appetite needs to stay below risk ***capacity***, which is the break-point for an organization before risk events cause results from which no recovery may be expected.
- Risk tolerance measures and key risk indicators help management quantify risk capacity, appetite, and tolerance.
- The terms "risk tolerance measures" and "key risk indicators" are sometimes used interchangeably. However, risk tolerance measures refer specifically to the *boundaries* of acceptable variations in performance related to achieving objectives, while risk indicators are *metrics* that help identify changes to the risks themselves.

The Framework



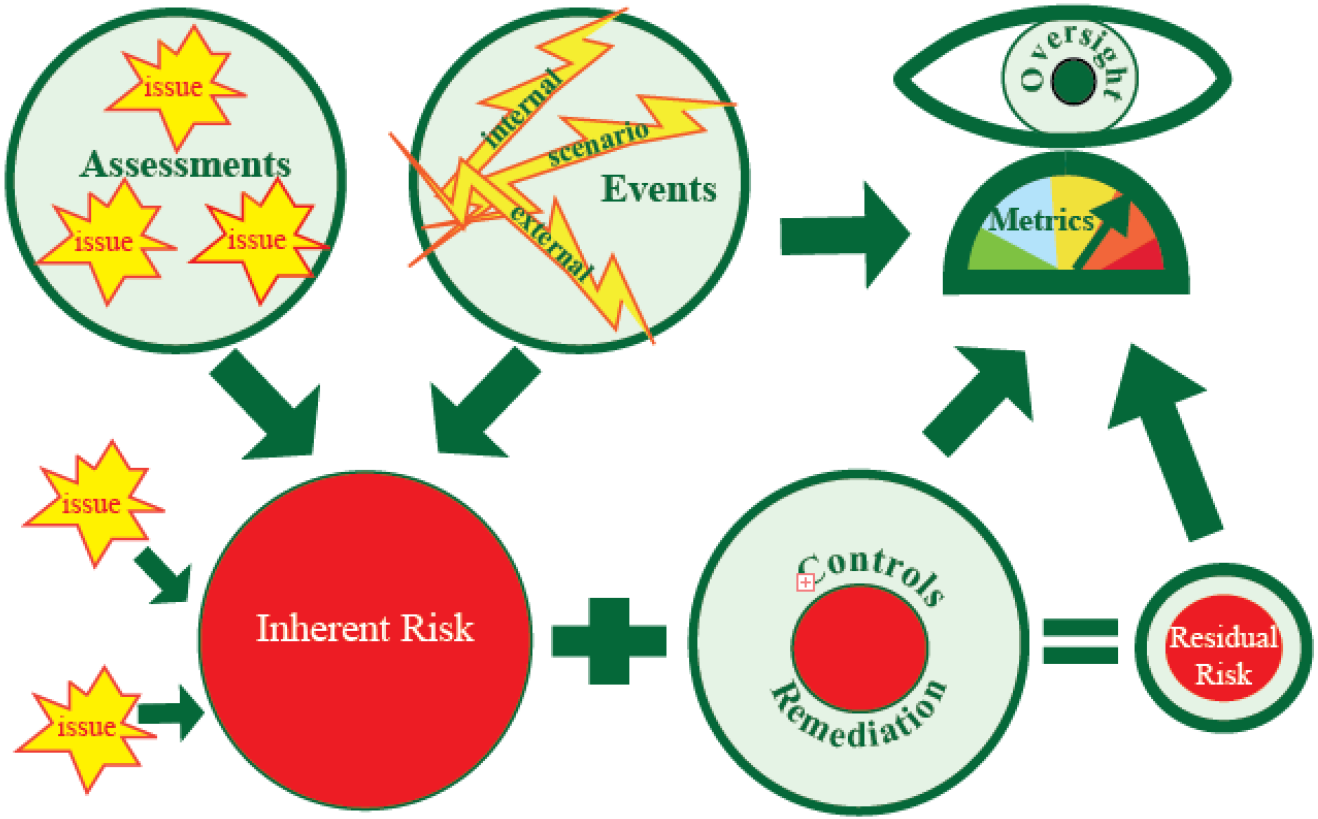
What the Framework is Not



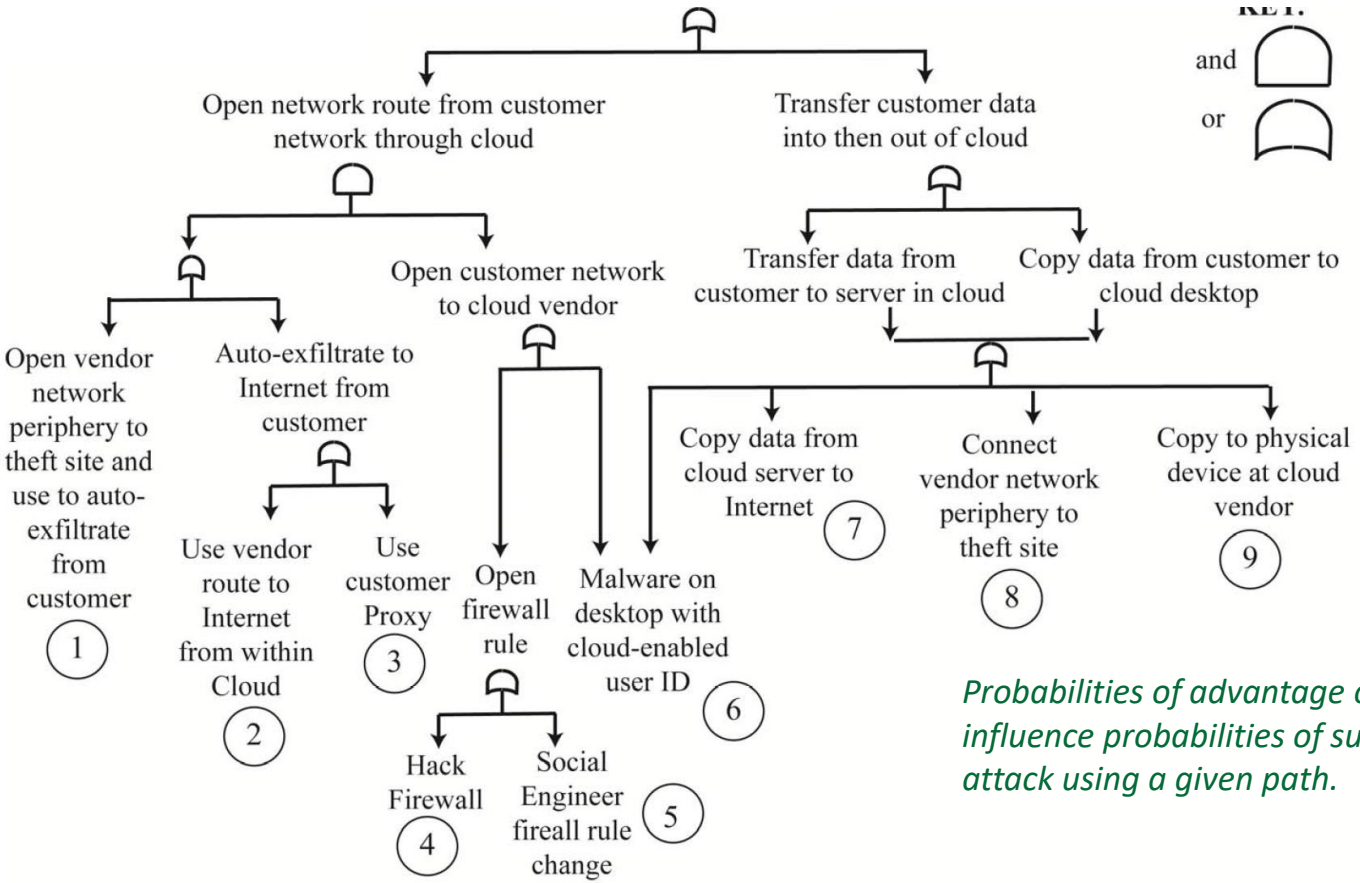
The Framework is not a NEW method of managing multiple assessment projects.

It encompasses the existing practices designed to collect information needed for Cybersecurity Risk Management.

Framework Cliff Note Version



A Common Approach to Risk Assessment



Probabilities of advantage of each step influence probabilities of successful attack using a given path.

A Common Sense Approach to Estimating Likelihood of Attack, Given Tree

If attacker is insider, probability of success increases.

Probability ("P") of Attack Success =

P(Workstation) = 1 – as everyone has access to their own workstat

```
* Max {
        Max {
                P(Network) = 1 IF internal network admin attacker
                P(Network Vulnerability)
        }
        Max {
                P(Operating System) = 1 – IF internal OS admin attack
                P(OS Vulnerability) – IF internal attacker
                P(Network) * P(OS Vulnerability) – IF external attacke
        }
        Max {
                P(Application) = 1 – IF internal application support at
                P(Application Vulnerability)
        }
        Max {
                P(Database) = 1 – IF internal database admin attacke
                P(Database Vulnerability) – IF internal attacker
                P(Network) * (Database Vulnerability) – IF external att
        }
}
```

Probability ("P") of Attack Success =

```
{
  P(Workstation) = 1
   * MAX {
      P(Network) = 1 (if net admin)
      P(Network Vulnerability)
    }
   * MAX {
      P(OS) = 1 (if OS admin)
      P(OS Vulnerability)
    }
   * MAX {
      P(Application) = 1 (if App Supp)
      P(Application Vulnerability)
    }
   * MAX {
      P(Database) = 1 (if DB admin)
      P(Database Vulnerability)
    }
}
```

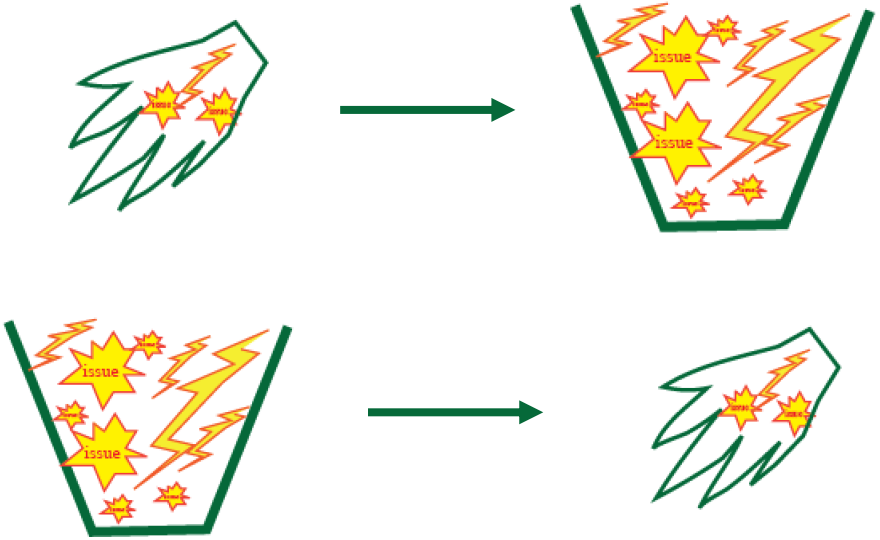
Probability of Success, Given Collusion

Attacker:	External	Internal	NW Admin	OS Admin	App Support	DB Admin	NW&OS
Probability of Attack Success Case (a):							
P(Workstation)	100%	100%	100%	100%	100%	100%	100%
Network	10%	10%	100%	10%	10%	10%	100%
Operating System	5%	50%	50%	100%	50%	50%	100%
Application	75%	75%	75%	75%	100%	75%	75%
Database	6%	60%	60%	60%	60%	100%	60%
OVERALL PROBABILITY FOR ROLE:	75%	75%	100%	100%	100%	100%	100%
Probability of Attack Success Case (b):							
P(Workstation)	100%	100%	100%	100%	100%	100%	100%
Network	10%	10%	100%	10%	10%	10%	100%
Operating System	5%	5%	50%	100%	5%	5%	100%
Application	4%	4%	38%	75%	100%	4%	75%
Database	2%	2%	23%	45%	60%	100%	45%
OVERALL PROBABILITY FOR ROLE:	10%	10%	100%	100%	100%	100%	100%

issue

Statistics versus Probability

Statistics: Given the information in your hand, what is in the pail?



The previous example was looking at the hand.

Probability: Given the information in the pail, what is in your hand?

Once source for the pail: Verizon DBIR

How to extrapolate from the pail?

DBIR data lists attacks by category, in a given industry, but internal factors also influence this, so it must be used in *combination with event attributes* that can be compared to internal ones, such as controls and issues.

ID	Type	Summary	Severity	Org
DBIR-1	External	Use of Stolen credentials		FIU
DBIR-2	External	RAM scraper		FIU
DBIR-3	External	Phishing		FIU
DBIR-4	External	Privilege abuse		FIU
DBIR-5	External	Misdelivery		FIU
DBIR-6	Internal	Use of backdoor or C2	?	FIU
DBIR-7	External	Theft		FIU

"Undetermined", "Negligible", "Exposure", "Adversity", "Disaster"

Data source: Verizon DBIR, 2017

FRAMECYBER FED

Assessment: A000010: CF NIST-CSF-

Assessment Workpapers | Issues | Events | Ris

Requirement *ID.BE-2*

IDENTIFY

Business Environment

The organization's mission, objectives, stakeholders, and activities

Informed

The organization's place in critical infrastructure and its industry sector is identified and communicated

Filter List | Next | Prev

Reference	Status	Section	Su
ID.AM-5	ToDo	IDENTIFY	Asset Man

Requirement Identifier

Document Section

Document Subsection

Scale

Document section "grouping strategy", category, or classification

Full Text of Requirement

Assessor Evaluation of the Extent to Which the Requirement is Met

Observations

- Meets
- Compensates
- Planned
- NotMet
- N/A

- Flag Issue

Add issue

Assessor Indication of Whether the Assessment Should Report a Compliance Issue

Person within the Organization that Most Closely Manages the Business Proces That May Reasonably Be Expected to Maintain Control Over Compliance with Requirement "Control Owner"

Manege (E000022)

E000022

The Risk Department is developing training to ensure that all staff are aware of the role of their job function and business process with respect to national critical infrastructure.

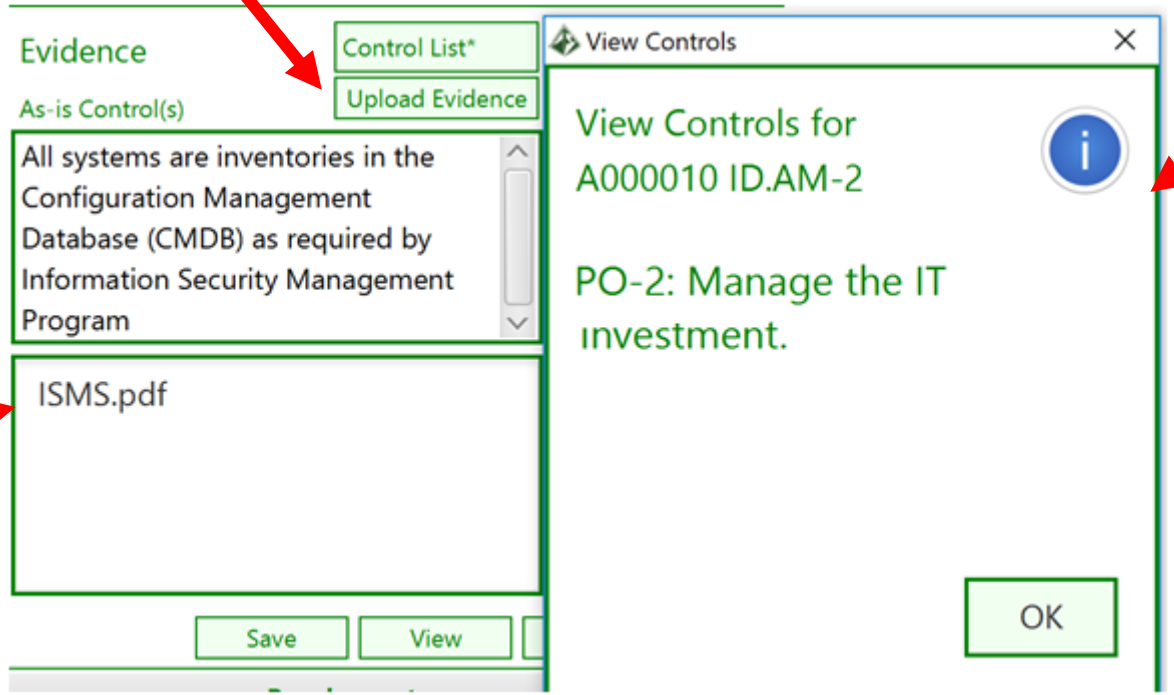
Free Form Documentation of Assessor Observations

Free Form Description of Available Evidence

Archive documented evidence.

Reference to existing control documents.

Reference to archive of documented evidence.



Recommendation

Free Form Assessor Recommendation

Create device inventory when the device is received by the Procurement Department, then hand-off to administrators for further details.

Maintain accountability for assessment data entry.

Updated on: 2019-03-20

by: Jones (E000001)

An Assessment Requirement Met

Difference is no issue

FRAMECYBER FED E000001

Assessment: A000005: CBT NY-DFS-500 Essey (E000007)

Assessment Workpapers | Issues | Events | Risks | Analysis | Controls | Enterprise | Metrics | People | Profile | ?

Requirement *500.02-a*

Cybersecurity Program

Security Program

Security Program

June 1, 2017

Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems, consistent with the defintion of Information System as a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing,

Observations

- Meets
- Compensates
- Planned
- NotMet
- N/A

Flag Issue

Add issue

Owner: Secoff (E000010)

Secoff (E000010)

By policy, the Chief Information Security Officer must implement design and implement a customized information systems security program. Details are attached.

Evidence

Control List* | Document | Documents

Upload Evidence

As-is Control(s)

ISMS.pdf

Recommendation

N/A

Updated on: 2019-03-15

by: Jones (E000001)

Filter List | Next | Prev

Save | View | Report | Convert | Export

Reference	Status	Section	SubSection	Requirement
500.02-a	Meets	Cybersecurity Program	Security Program	Cybersecurity Program. Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, inte
500.02-b	Meets	Cybersecurity Program	Security Program	The cybersecurity program shall be based on the Covered Entity's Risk Assessment (as defined in section 500.09) and designed
500.02-b.1	Compensating Control	Cybersecurity Program	Security Program	Core cybersecurity functions include: identify and assess internal and external cybersecurity risks that may threaten the security

Issue Summary

Source

Severity

Assessments | Issues | Events | Risks | Analysis | Controls | Enterprise | Metric KRIs | People | Profile | ?

Issue ID: I2

Summary: GDPR requirement: GDPR-CPO-25-1

Severity: Medium

Status: Open / Draft / Closed

Source: Assessment

Source ID: A000003-GDPR-CPO-25-1

Org: CBT

Created on: 2019-01-25

Target Date: 1/25/2019

Owner: Cio (E000003)

Last update by Jones (E000001) - 2019-03-11

Description

GDPR compliance is at risk due to current inability to fully anonymize data when sharing across applications. A compensating control is consent, however, consent processes may not meet deadline.

Project Information:

IT OMO # 1238 A Data Masking Server - Project to facilitate anonymization services across multiple applications

Criteria:

Plans to Meet GDPR assessment requirement: Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the

Plan to Remediate

Date to Remediate

Assessment Requirement

What

How

Impact Classification

Event ID: SOC-00451 Proxy Misuse

Impact Severity: Negligible

Business Process

Physical plant HVAC maintenance outsourced to HVAC supplier. Maintenance of heating, air conditioning, rack cooling, humidity control and other environmental factors. Monitored by Corporate Infrastructure Services.

Impact:

Disclosure of personally identifiable data resulting in customer notifications.

Currency/ Loss (if any) $ 32,000 Change Loss Calculation... Add issue Last update by: Jones (E000001) on 2019-03-06

Evidence of Loss

Tracking Accountability

Selecting Measures, Metrics and Key Risk Indicators

Measures, aka Base Measures, Primitives

ID: CRIT-Servers
Name: Critical Servers
Category: Measure
Source: Configuration Management Database (CMDB)
Scope: Servers that are used by critical applications
Algorithm: Count
Interval: Daily
Unit: Server

ID: HARD-Servers
Name: Hardened Servers
Category: Measure
Source: Host Security Software Database (HSSDB)
Scope: Servers that have standard security configuration
Algorithm: Count
Interval: Daily
Unit: Server

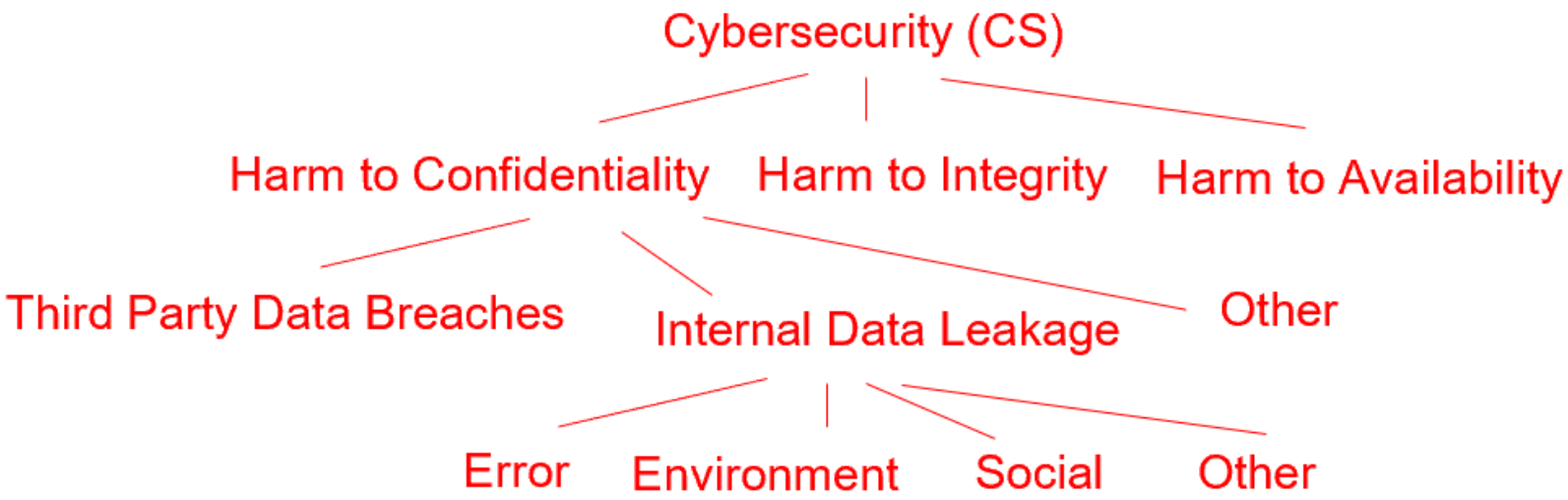
Metrics → Key Risk Indicators

ID: Server-Sec
Name: Server Security
Category: Target
Description: Percent of servers with secure build
Scope: CRIT-Servers
Algorithm: HARD-Servers/ CRIT-Servers
Interval: Daily
Unit: Percent

Events are Realized Risks and Therefore always Key Risk Indicators

ID: Breaches
Name: Data loss incidents within the enterprise
Category: Deterministic
Description: Number of events wherein confidential data was exposed
Scope: Enterprise
Algorithm: Count
Interval: Continuous
Unit: Event

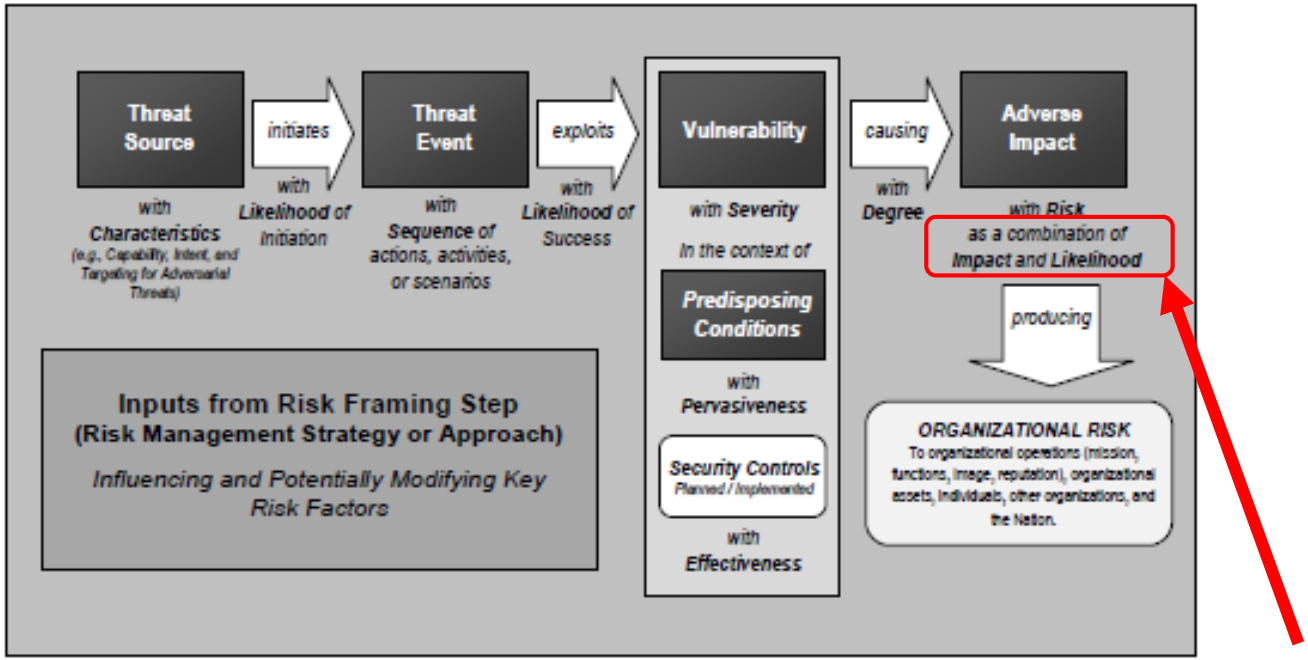
What does the pail look like?



Event types =*def* risk categories,
and have characteristics similar to an attack tree.

However, events may overlap categories….

NIST Minor Deviation from Standards



Note that COSO and COBIT measure risk in probability and describe and event spectrum from opportunity to negative consequences.

[1] *NIST SP800-30, Guide for Conducting Risk Assessments*

Risk Assessment

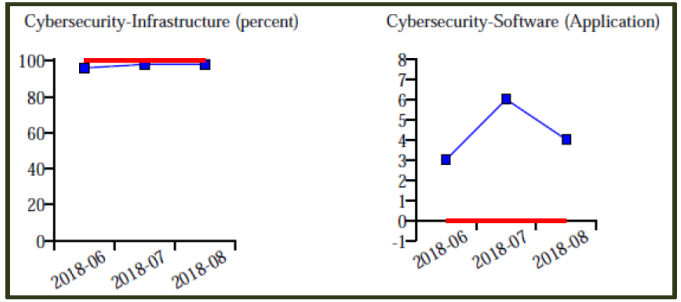
Report for Risk Category: Harm to integrity

Risk Category is Sourced from Document Firm Top Ten Risks (TopTen)

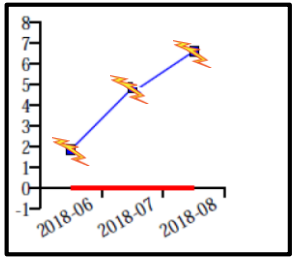
Key Risk:	Yes
RiskAppetite:	The firm has no tolerance for events that stem from known vulnerabilities in its systems.
Inherent Risk:	High
Residual Risk:	Medium
Likelihood:	100%
Controls:	CS-Policy, Owner: The Ciso (E000002): Cyber-1.1: Information Classification: Record Sets, All information used for official business must belong to a Record Set of CI, AAI, PII, NPII, MNI, CNPI, FI, SNPI, or ISPI, according to its contents as defined herein., Identify, Policy, As Needed CS-Policy, Owner: The Ciso (E000002): Cyber-4.1: Technology Control Standards: Control Standards, Comprehensive technology control standards must be maintained that cover all platforms and services, including the activities listed in this section., Identify, Policy, As Needed CS-Policy, Owner: The Ciso (E000002): Cyber-5.1: Technology Control Standards: Monitoring, Standards compliance must be monitored, and deviations promptly addressed by the Technology Management Committee. Instances of repeat non-compliance must be escalated to the Risk Committee., Identify, Policy, Continuous OS-Hard-SW, Owner: The Cio (E000003): OSHS-Harden-9: Manifest change detection, Incident response procedure includes reviewing logs and identifying root cause of changes in Manifest configuration., Detect, Procedure, As Needed
Metrics:	SecurityAutomation - OS Security Software Performance Percent of servers sending updates to OS Security Server (Target) Algorithm: =ACT-Servers/HARD-Servers KRI: Cybersecurity-Infrastructure (KRI): Indicator reflects security of technology infrastructure. Threshold: 0.9999 Comparison: Below threshold SevereVuln - Severe Vulnerabilities in Internet-facing Applications Number of applications with severe vulnerabilities (Vulnerability) Algorithm: =unique(intersection(EXT-Apps,CVE).Application()) KRI: Cybersecurity-Software (KRI): Indicator reflects security of externally-facing software. Threshold: 0 Comparison: Above threshold
Issues:	AUD435: File integrity monitor disabled - New software acquisition process inadvertently cancelled license for integrity monitor and new software is not yet deployed and tested. *Source: Audit-IA-FIS-435 (FIU)*
Events:	Internal (WTG): 1 - Wire Transfer Fraud Wire Transfer operator employee used stolen authentication to transfer customer funds to a relative's account
Category:	TopTen (CRO): CS - Cybersecurity - Intentional harm to systems confidentiality, integrity, and availability due to actors with malicious intent

What metric is the best match between your organization and the pail?

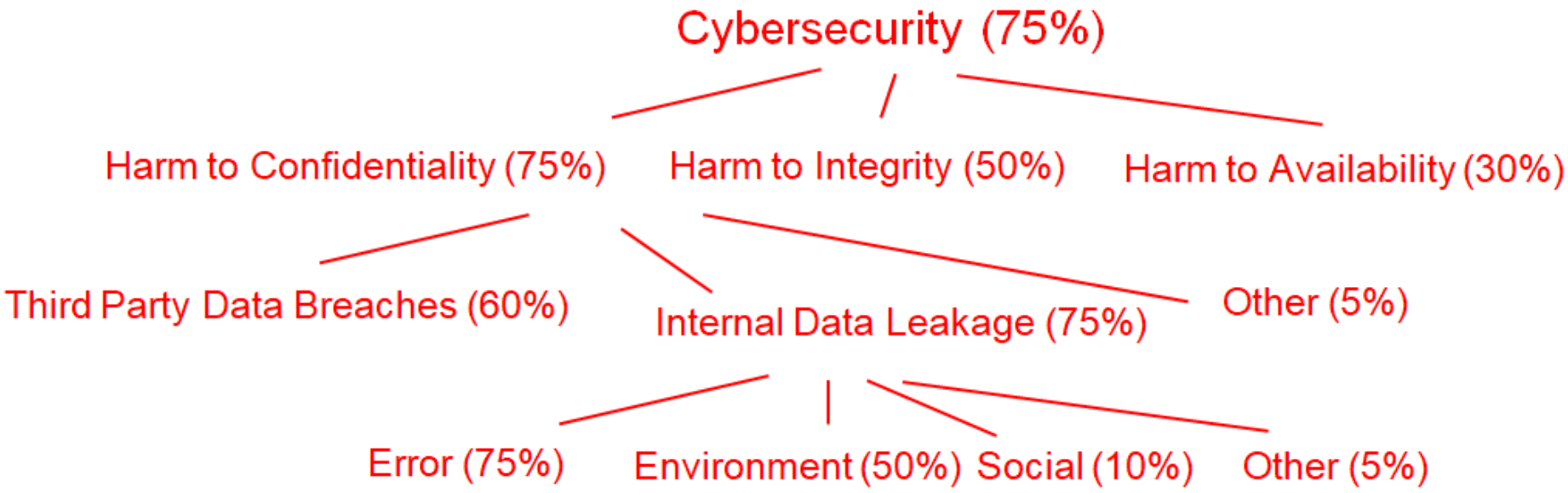
Key Risk Indicators



Note actual events always tip the probability to 100%



On which nodes does your organization look like the pail?



Note the aggregate is the highest probability among sub-categories.

NIST Warning:[1]

CAUTIONARY NOTES

SCOPE AND APPLICABILITY OF RISK ASSESSMENTS

- Risk assessments are a key part of effective risk management and facilitate decision making at all three tiers in the risk management hierarchy including the organization level, mission/business process level, and information system level.
- Because risk management is ongoing, risk assessments are conducted throughout the system development life cycle, from pre-system acquisition (i.e., material solution analysis and technology development), through system acquisition (i.e., engineering/manufacturing development and production/deployment), and on into sustainment (i.e., operations/support).
- There are no specific requirements with regard to: (i) the formality, rigor, or level of detail that characterizes any particular risk assessment; (ii) the methodologies, tools, and techniques used to conduct such risk assessments; or (iii) the format and content of assessment results and any associated reporting mechanisms. Organizations have maximum flexibility on how risk assessments are conducted and are encouraged to apply the guidance in this document so that the various needs of organizations can be addressed and the risk assessment activities can be integrated into broader organizational risk management processes.
- Organizations are also cautioned that risk assessments are often not precise instruments of measurement and reflect: (i) the limitations of the specific assessment methodologies, tools, and techniques employed; (ii) the subjectivity, quality, and trustworthiness of the data used; (iii) the interpretation of assessment results; and (iv) the skills and expertise of those individuals or groups conducting the assessments.
- Since cost, timeliness, and ease of use are a few of the many important factors in the application of risk assessments, organizations should attempt to reduce the level of effort for risk assessments by sharing risk-related information, whenever possible.

Where we can help

[1] *NIST SP800-30, Guide for Conducting Risk Assessments*

Questions?
Discussion

jennifer@bayuk.com

www.Bayuk.com
www.framecyber.com