Successful Matchmaking of NIST 800-63-3 Digital Identity Guidelines and Monetary Risk using the FAIR Standard

A real world reflection of user authentication, risk, cost, and implementation as the two cyber standards work together.

September 13, 2017

BLOCK, CHIP
Evolver Inc.

Successful Matchmaking of NIST 800-63-3 Digital Identity Guidelines and Monetary Risk using the FAIR Standard

A real world reflection of user authentication, risk, cost, and implementation as the two cyber standards work together.

I have just completed an initial review of the recently released NIST Special Publication 800-63-3, Digital Identity Guidelines, and, after a bit of thought, have come to realize how important this document is to both government and commercial organizations. The document release got a lot of press because it changed the recommendation for the creation of passwords (emphasized by recent regrets of the originator of the current password guidelines). In reality, this was a very minor element of the publication.

As I walked through how an implementation of this publication would be executed, another critical element became apparent. The new 800-63-3 publication and the monetary quantification of cyber risk provided by the Factor Analysis of Information Risk (FAIR) model were made for each other.

The Digital Identity Guidelines (800-63-3) publication has a really insightful paragraph in the executive summary about identity and accessibility of online systems.

> *Digital identity as a legal identity further complicates the definition and ability to use digital identities across a range of social and economic use cases. Digital identity is hard. Proving someone is who they say they are — especially remotely, via a digital service— is fraught with opportunities for an attacker to successfully impersonate someone. As correctly captured by Peter Steiner in* The New Yorker*, "On the internet, nobody knows you're a dog." These guidelines provide mitigations to the vulnerabilities inherent online, while recognizing and encouraging that when accessing some low-risk digital services, "being a dog" is just fine; while other, high-risk services need a level of confidence that the digital identity accessing the service is the legitimate proxy to the real-life subject.*

This inability to distinguish between identity proofing and accessibility has led to either highly vulnerable systems or extremely expensive and wasteful security implementations often confusing authentication with authorization. Organizations either use weak username password single sign on or they make everybody in the organization buy hardware tokens that costs millions of dollars to purchase and costs even more to maintain. Neither of these approaches meet the needs of securing the organization.

Identity and Risk

What the new publication recognizes is that identity and authorization are a function of risk. The document even states "*These guidelines describe the risk management process for selecting appropriate digital identity services and the details for implementing identity assurance, authenticator assurance and federation assurance levels based on risk."* The publication then lays out a well-defined process based on three components, Identity Assurance Level (IAL), Authenticator Assurance Level (AAL), and Federation Assurance Level (FAL).

I won't go into details of these areas but I recommend a review of the document to see how these levels are combined to determine the critical questions of "Should I use one factor or two factor security? Do I need to have identity proof of the users? Can I use two factor such as SMS messaging or do I need a hardware authenticator?"

The Department of Defense is leaving CAC/PIV cards for a variety of reasons and other agencies and organizations are also looking at their authentication approaches. This raises the question, for the many levels of sensitivity and releasability of information: is a single or multiple approach needed and based on what?

FAIR and the Implementation of 800-63-3

As I read the new publication, the alignment with the monetary quantification of risk becomes fairly obvious. As many know, FAIR is the open standard being adopted across commercial and government organizations to determine cyber risk in monetary terms. To explain how FAIR and the Digital Identity Guidelines align, a hypothetical use case is the best method.

FAIR and Digital Identity Use Case Scenario

Let's say a large organization with 10,000 employees is reviewing its identity and authorization program. A recent cyber audit has found that secure access to critical systems was lacking. Most of the current systems are username/password protected without any second form of authentication. Most passwords have not changed in years, if ever.

Before FAIR and 800-63-3

Senior management has been presented with the following identity and authorization options based on current approaches:

1.) Leave the current system in place and hope nothing bad happens

Result – extremely high risk of breach or loss of production/dollars from a cyber attack

2.) Implement a card based/token two factor authorization for all employees logging into organization systems

Result – extremely expensive and major impact on productivity and efficiency of employees. Potentially marginal risk reduction based on implementation.

In addition to the technical requirements needed for implementing a hardware token approach, a major cost is incurred in doing background checks on large numbers of employees to validate their credentials, even though they may not regularly access critical systems. Experience has also shown that these type of hardware authentication programs are extremely expensive to maintain as detailed tracking of every

card is required. This includes replacing lost and broken cards, deprecating employees' cards that leave the company, and generating new cards for new and transferring employees.

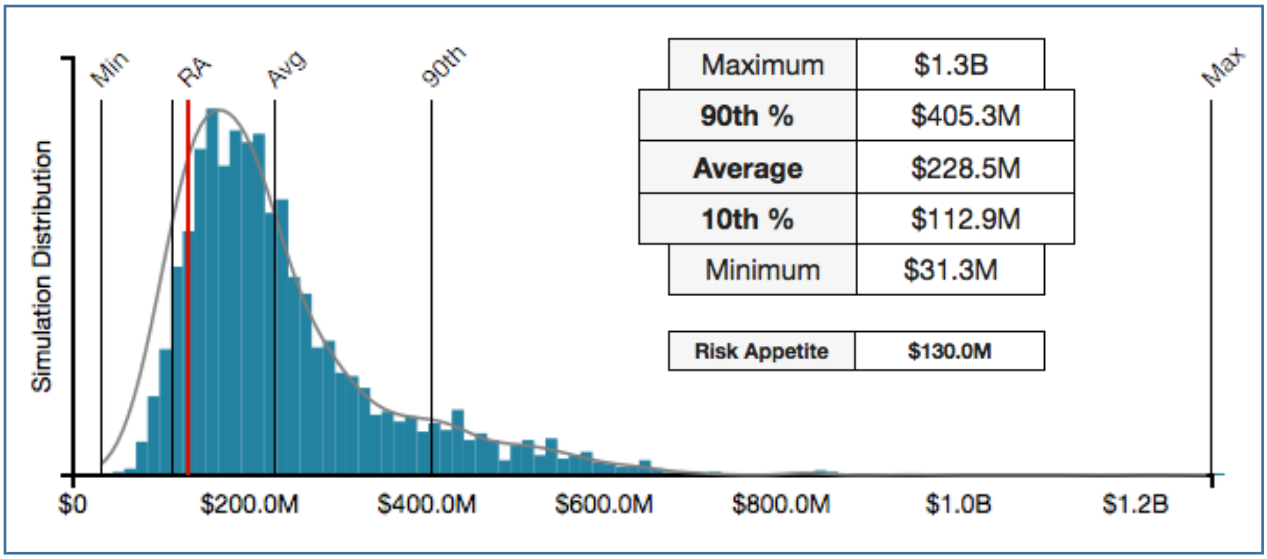
An average yearly cost of ownership of a hardware based two factor authentication solution of $200/user is not unusual, amounting to $2M per year for the organization. Additionally, the training of staff, updating systems, developing new policy documentation, and other initial implementation activities will cost the company another $1M. Overall, the program has a $3M first year investment and an ongoing $2M per year expense.

When presented to the Board of Directors, the obvious question was asked: "How much more secure will we be after spending all of this money?"

Applying FAIR

A combination of the FAIR monetary cyber risk model and 800-63-3 provides both an effective approach and an answer to the Board of Directors question. Here is how:

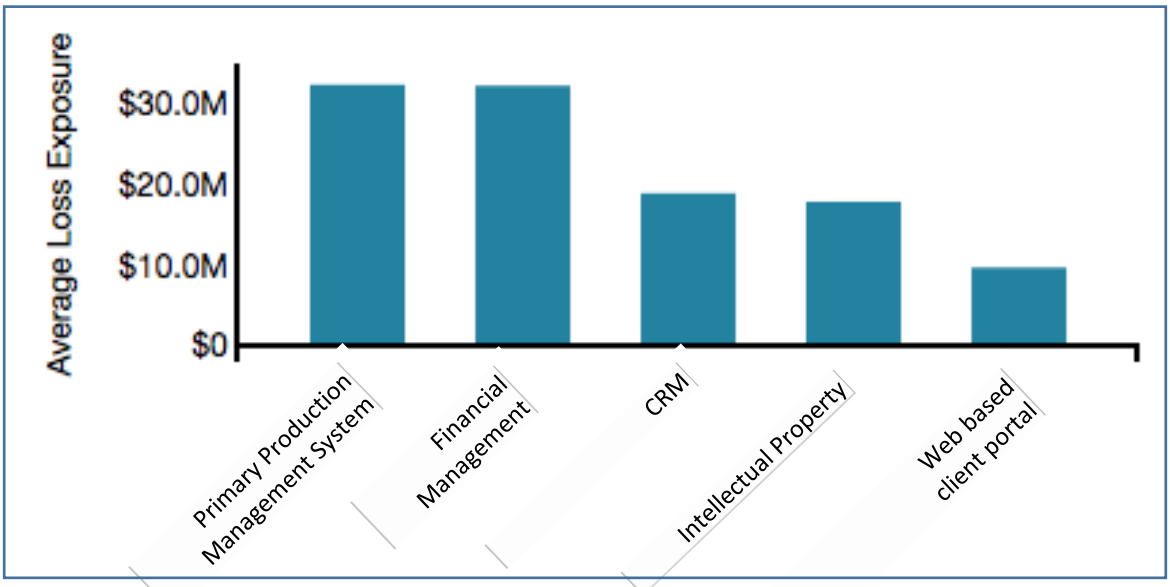
The first step is a FAIR analysis of the primary systems of the overall company. The results of the analysis shows that the current yearly Average Loss Exposure (ALE) for the company, using the RiskLens™ tool, is $228M dollars, as shown in the following chart.



A deeper dive into the FAIR analysis shows that of this risk, there is a strong concentration of risk around five primary asset areas.

Those areas are:

1. Primary production management system
2. Customer resource management (CRM) system
3. Financial management system
4. Intellectual property storage system
5. Web based client portal



From this analysis, the systems that need the most protection are identified in a monetary method which also shows the CISO and others where tight identification and authorization are most important. Further analysis would show that the total number of users for the first four systems is less than 500. The last system, the client facing portal, has a large number of users, but the question for this system becomes what form of authentication is the most effective?

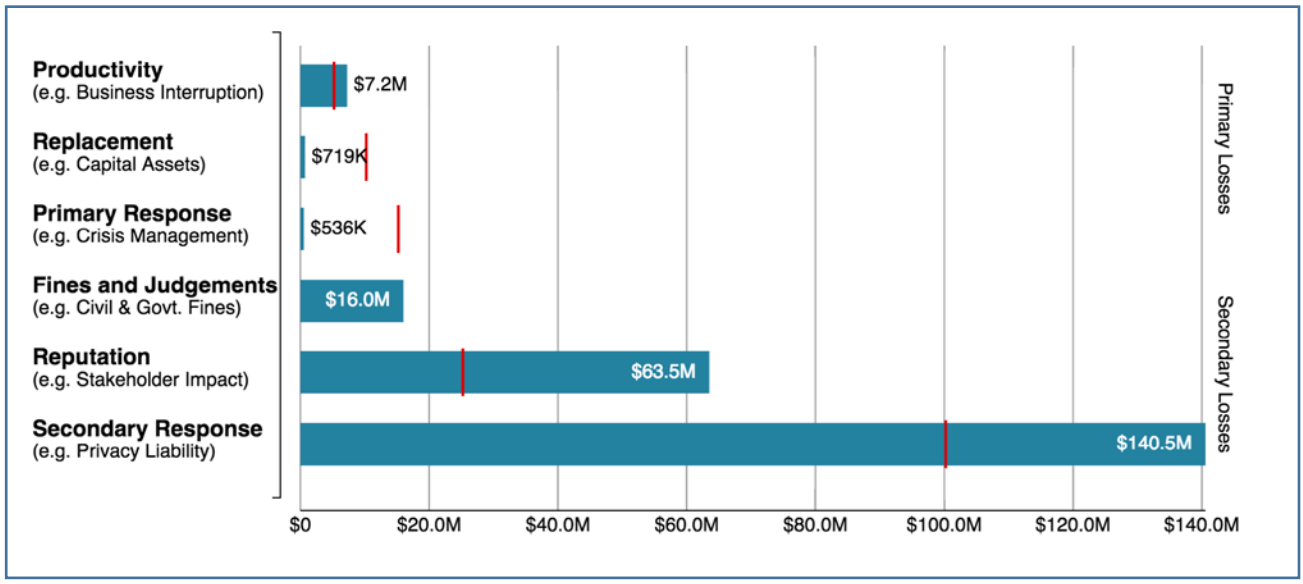
The 800-63-3 guideline provides a logical flow for determining the Identity Assurance Levels (IAL), the Authenticator Assurance levels (AAL) and the Federation Assurance Levels (FAL). Interestingly, the key questions posed by the guidelines align well with the results derived from a FAIR analysis.

A list from 800-63-3 of the main questions for determining IAL, AAL and FAL are:

Inconvenience, distress, or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	Low	Moderate	High
Unauthorized release of sensitive information	Low	Moderate	High
Personal safety	Low	Moderate	High
Civil or criminal violations	Low	Moderate	High

The results from each of the FAIR analysis shows these results in dollars and cents risks, therefore answering the questions posed by the 800-63-3 guidelines.

An example of the findings from FAIR analysis are below:



The 800-63-3 special report provides guidance, based on this information, as to what level should be utilized for the IAL, AAL and FAL for each asset area. The organization utilized the FAIR analysis and determines the following:

Primary production management system	Customer resource management (CRM) system	Financial management system	Intellectual property storage system	Web based client portal
IAL-3	IAL-3	IAL-3	IAL-3	IAL-1
AAL-3	AAL-2	AAL-3	AAL-3	AAL-2

From this analysis, the organization can now make two factor authentication implementation decisions based on real data, not just conjecture. After analyzing all of the information, the organization decides the following:

Applying 800-63-3

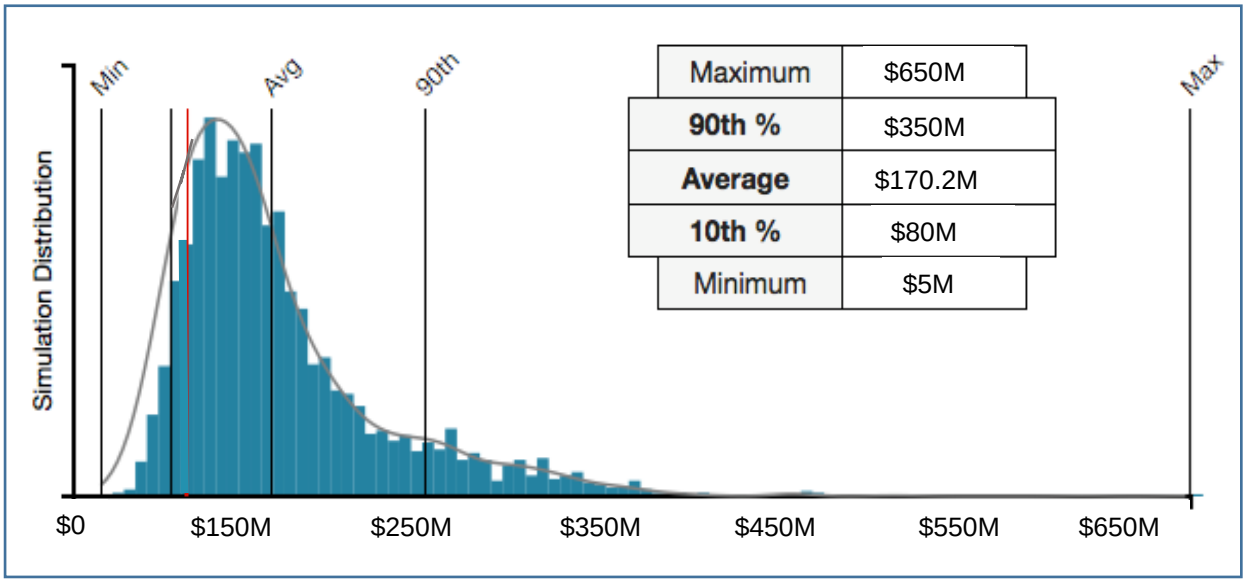
Two factor authentication with hardware authenticator for the primary production management system, financial management system and intellectual property storage system with background checks of each user.
Total users – 500

Two factor authentication without hardware authentication requirement for CRM system with background check on all users.
Total users – 50

Two factor authentication without hardware authentication for web based client portal with no in person validation of identify required.

With this approach, a new FAIR analysis can be run utilizing the improved security features to show what the likely reduction in risk, in monetary terms, will be achieved by the organization. It can also be readily adjusted as newer metrics or solutions are introduced.

The new FAIR analysis using this identify approach shows a $50M reduction of ALE for the organization due to the increased security achieved across the five primary risk areas.



Maximum	$650M
90th %	$350M
Average	$170.2M
10th %	$80M
Minimum	$5M

Briefing to the Board of Directors with Tangible, Financially Based Risks and Options

Unlike the first scenario where the board was briefed of a major expense with little quantification of the results, the use of FAIR and the 800-63-3 dramatically changes the discussion. Not only has the overall

cost of implementation been dramatically reduced, but there is an estimate of risk reduction based on the investment.

The resulting brief would now go like this:

Resulting brief utilizing 860-63-3

Two factor authentication with hardware authentication for 550 users
Cost -$110,000.

Initial implementation $500,000.

First year cost, $610,000 with $110,000 ongoing costs

Two factor authentication with soft token (SMS messaging, email response) for 10,000 users. Costs - $20/user - $200,000

Total Cost - $800,000 with ongoing cost of $110,000

Estimated reduction of Annualized Loss Exposure (Risk) - $50M

This briefing provides information that the board of directors can use to make logical, financially based decisions.

Authentically Analyzing Trade Offs in Cybersecurity Investments

Using methods such as the one reflected in this example use case, other trade off analysis can be conducted such as determining the value of doing in person identity verification of CRM users or if using soft tokens with CRM would be a good investment. If the Board asks questions, fact and probability-based answers can be given. Flexible "what if" drills can be nearly instantaneously conducted to best understand trade-offs. Third-party risks can also be incorporated, e.g., hardware/software vendors risk absorption to obtain a best mix of solutions without introducing further risks for the responsibility of the organization.

Overall, the organization is making logical decisions around identify and authentication based on a defendable metric (money) that is understood by all involved. The emergence of the Digital Identity Guidelines from NIST and the use of the FAIR model as a de facto standard for monetary quantification makes for the perfect match. Identify and authorization is the cornerstone of any security program and by providing decision makers with clear, understandable investment strategies, the board is no longer faced with that scary statement "it will cost a lot and we *hope* it will be better." Instead, they are presented with a reasonable cost and an expected amount of reduced risk.

About the Author

Chip Block is Vice President of Evolver, Inc. a major supplier of cybersecurity and infrastructure services to the commercial and public sectors. Mr. Block has worked extensively in the cyber research, development and operations field for over fifteen years and been awarded several high level honors for his advanced technological achievements. He is a frequent speaker and author on cybersecurity, Internet of Things, cyber risk, and cyber insurance. In 2016, he was recognized as ACT-IAC's Individual Contributor of the year. His email is chip.block@evolverinc.com.