VERVE
INDUSTRIAL PROTECTION

WHITE PAPER

OT CYBERSECURITY MATURITY

A 5 STEP GUIDE TO USING THE NIST CSF

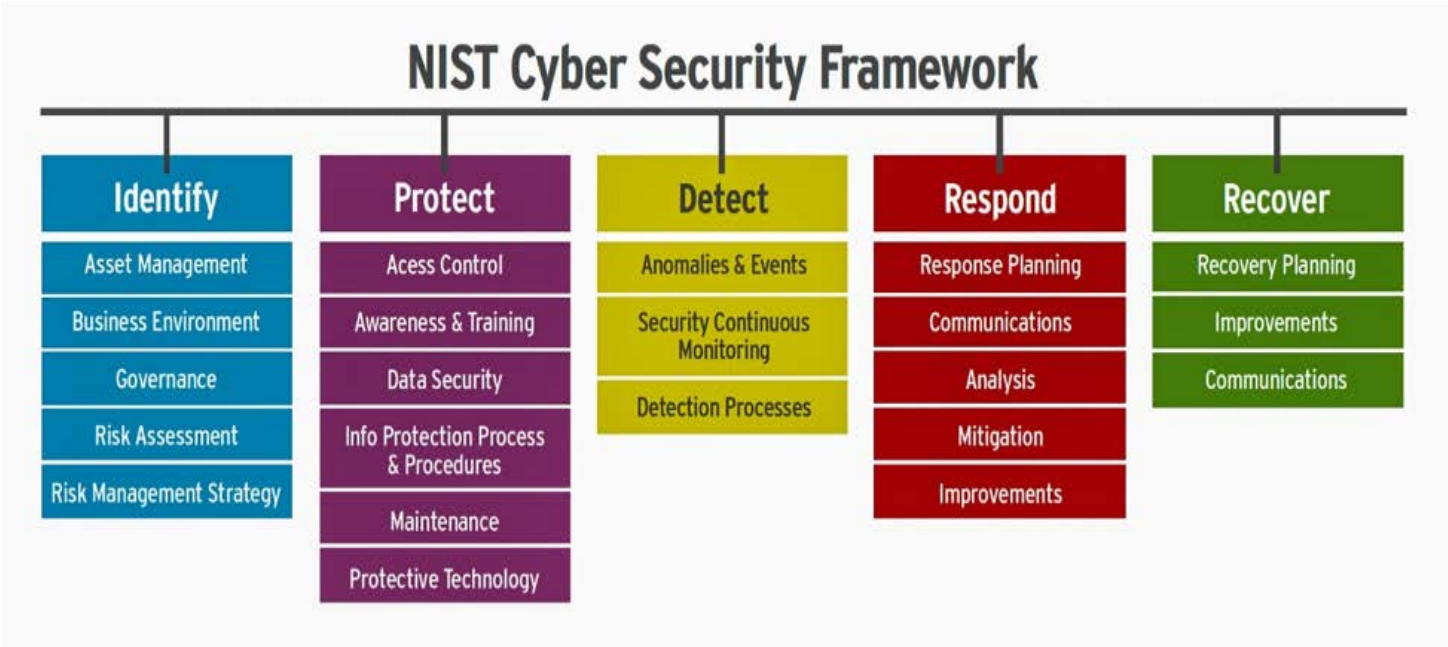
On April 23rd, NIST released Version 1.1 of the NIST Cyber Security Framework (CSF). The original NIST CSF has gained significant traction since its release in early 2014 – within its first two years Gartner estimated that 30% of organizations had already adopted some elements of the framework. Version 1.1 adds important new elements and clarifies original elements to help companies continue to advance their cybersecurity practices. This guide and the accompanying case study provide a roadmap to using the CSF to drive greater cybersecurity maturity in control systems.

Visit the URL for this White Paper at VerveIndustrial.com/white-paper.

NIST CSF VERSION 1.1

NEXT GENERATION OF CSF GUIDANCE

NIST CSF FRAMEWORK



Building on the success of NIST CSF v1.0, NIST recently released an updated version providing greater clarity, additional components, and further guidance. This "V 1.1", as it is called, has several key additions from version 1.0.

- Added focus on supply chain risks for both products and services. Particular emphasis in the "Identify" category on identifying who has access to your systems and managing those appropriately.
- Expansion of "access control" section to "Identity Control & Access Control" to identity management and authenticating identities.
- Added language to encourage and manage sharing of information through ISACs and other organizations with requirements to establish processes to receive, analyze and respond to internal and external identified vulnerabilities
- Added a section with more detail on measurement – i.e. quantitative measures of compliance with different levels of security maturity and how to establish those measures effectively.

What is clear from these additions is that the version 1.0 was comprehensive in its own right. The original NIST Framework has 5 Core elements: Identify-Protect-Detect-Respond-Recover. It refers to other standards such as NIST 800-53, etc. to provide more detailed guidance on specific functions.

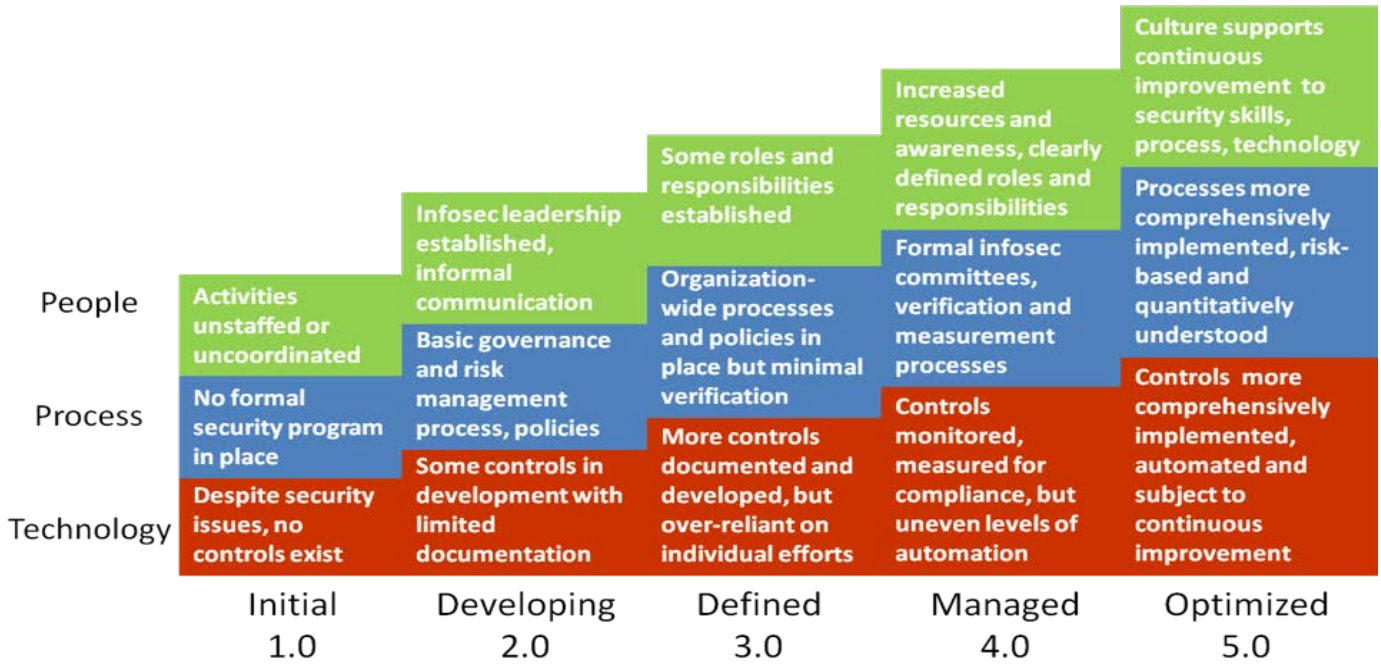
NIST CSF VERSION 1.1

NEXT GENERATION OF CSF GUIDANCE

PROFILES

It then includes "Tiers" which are not officially maturity levels, but do provide a framework to judge the level of advancement in automation and implementation. They range from Tier 1 (Partial) all the way to Tier 4 (Adaptive). As NIST states in its own description, "These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed."

Finally, the framework calls for users to establish "Profiles" which describe the current state of cybersecurity maturity against each category as well as the company's target objective for that category. These profiles are unique to each company and should be developed with an eye towards cost-benefit trade-offs.



The NIST CSF is much less prescriptive and complex than the full NIST 800-53 compliance standards which runs over 400 pages in print. As a result, it can also be tough to use as a guideline since there is so much left to the user to develop and shape.

We have worked with dozens of organizations on their cybersecurity maturity journeys. Based on that experience we have developed the below 5-step guide to significantly improve an organization's cybersecurity maturity, specifically focused on their operating control systems – sometimes referred to as ICS, OT, or IIOT.

A 5-STEP GUIDE TO GREATER MATURITY

CYBERSECURITY MATURITY IS NOT A DESTINATION, BUT A JOURNEY. EACH DAY ATTACKERS CREATE NEW ATTACK VECTORS, VENDORS FIND NEW VULNERABILITIES, AND DEFENDERS IDENTIFY NEW PROTECTIVE AND DETECTIVE MEASURES. COMPANIES CANNOT IMPLEMENT ALL CONTROLS DAY ONE. SO, HOW DO YOU BEGIN AND PROCEED LOGICALLY ALONG THAT MATURITY JOURNEY? WHAT DOES THE PROGRAM LOOK LIKE? THE BELOW 5 STEP GUIDE PROVIDES A ROAD MAP TO BOTH RAPID SIGNIFICANT MATURITY INCREASES AS WELL AS LONG TERM CONTINUOUS IMPROVEMENT OF MATURITY LEVELS.

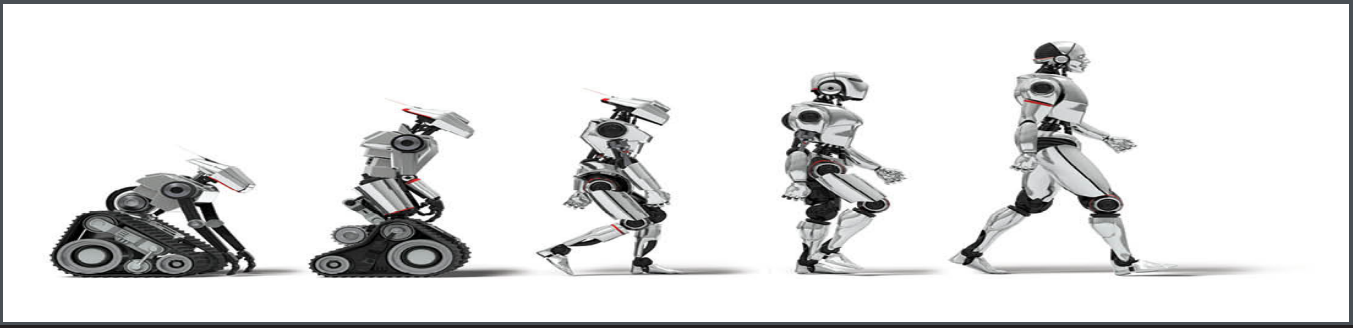
STEP 1: RAPID ASSESSMENT

It's hard to know where to go if you don't know where you are. The first step in following the NIST CSF is to establish a robust – but rapid – assessment of your current status. "Assessment" is a vague term, however. Many customers get stuck before the journey begins under the weight of an assessment process that turns into a months-long exercise in surveys, network diagram reviews, penetration tests, etc. The key to gaining momentum is to conduct a rapid assessment within 60 – 90 days across the organization. This rapid assessment process provides enough detail to build an initial maturity roadmap and to enable the company to begin to make progress. It is not intended to diagnose every threat pathway or end-point vulnerability.

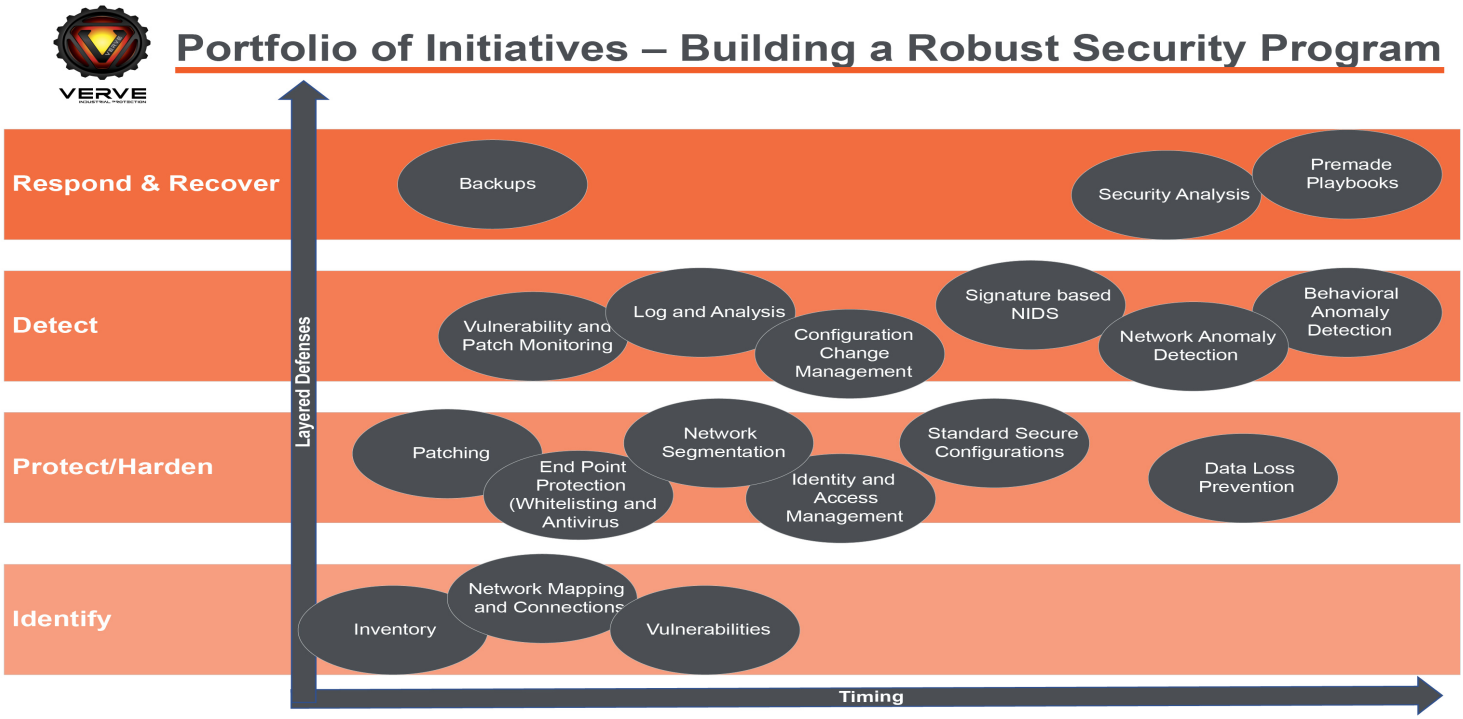
The rapid assessment should provide input on the cybersecurity baseline on people, processes & policies, and technology. It will typically encompass components:

- Agreement on the "Profiles" or levels that your company will establish for different stages of maturity. (An example is provided above).
- Brief surveys (Less than 50 questions) to key personnel in the organization
- Targeted interviews by people with experience in NIST CSF to round out the quantitative survey results

Together, these three components should be sufficient to build an initial assessment to help define the maturity roadmap.



STEP 2: TARGET MATURITY ROADMAP



Specific Security Controls Applied Over Time as Compared to the NIST CSF Categories

The assessment provides the baseline starting point, but the critical step is to then layout your company's cybersecurity maturity aspiration based on your specific business needs, regulatory requirements, etc. and build a robust roadmap based on a portfolio of initiatives across process development, technology deployment, and training & awareness.

To develop a successful roadmap, the following should be considered:

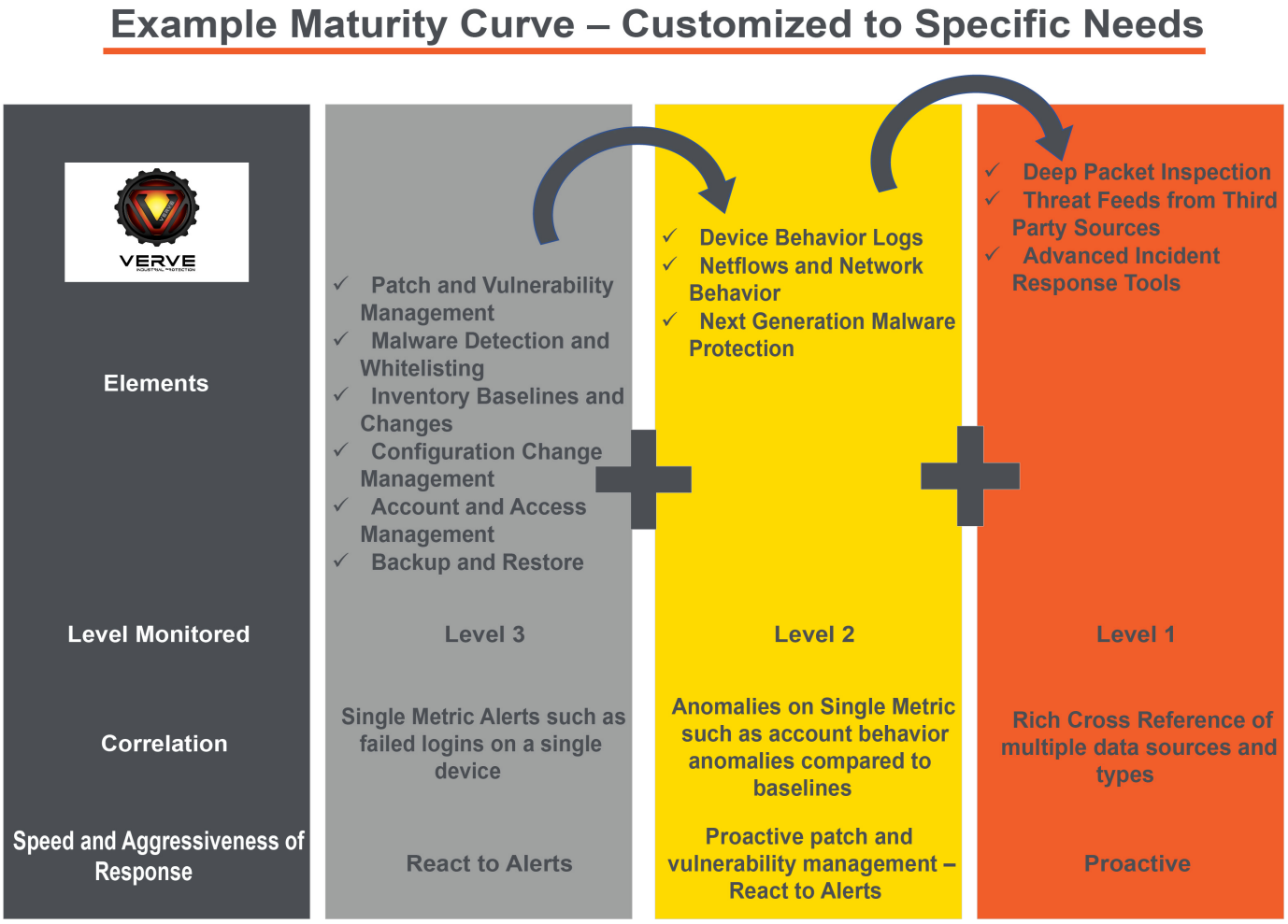
- Sequence of initiatives/foundational elements: Certain initiatives are pre-requisites of others. For instance, having a complete and detailed hardware and software (OS, firmware, application software, configurations, ports, services, etc.) inventory is a requirement to harden configurations and many other CSF categories
- Prioritization based on business needs, risk & budgets: Based on the assessment, specific initiatives will raise in priority because they pose the greatest threat to the business operations. The assessment should provide the core information necessary to prioritize the greatest risk to the organization. Obviously, this needs to be balanced against overall budgetary constraints.
- Measurement & Tracking: In parallel to any defensive or detective initiatives, the organization should build an ability to track and measure progress. The measurement category added to version 1.1 emphasizes the need for this.
- Integrating technology, people and process: Implementing technology without the people or processes to support it will lead to wasted investments. Similarly, without technology, the procedures the company may develop may be too onerous to provide much insight to the cybersecurity situation.
- Integrating platform (or "glue"): Over time the number of initiatives, technology and procedures will grow. Without careful consideration to investment in the overarching platform or glue that ties these pieces together, the program may become overwhelming.

TARGET MATURITY ROADMAP (CONT)

EXAMPLE MATURITY CURVE

Taken another way, the need to build on the portfolio of initiatives is usually executed in a cyclical fashion over multiple discrete projects and budgets. The objective is to move from the basic level of protections through higher levels of sophistication and an eventual shift from reactive to proactive monitoring and detection as depicted in the maturity cycle below.

MATURITY CYCLE



It is important to note that the above cycle is just a general intended pattern towards a more robust security program. The specific tasks, the order they are executed and the time frame across which they are deployed absolutely have to be tied to the specific risks and objectives of the individual organization.

STEP 3 - EXECUTE FOUNDATIONAL INITIATIVES

As discussed above, in almost every program there are a set of foundational initiatives that are necessary to enable the broader program. These initiatives should provide some rapid impact in security while also providing baseline capabilities. This first "wave" of initiatives should be items that can be achieved within 90 days to demonstrate progress as well as allow for rapid movement to additional elements. These initiatives will include both "informational" or "baselining" initiatives as well as the first wave of "remediation" or "hardening" activities. The baselining-type of activities would include things such as hardware and software inventory, configuration baselines, firewall rule maps, etc. The remediation-type activities would likely include software removal, hardening of baselines, initial segmentation, etc.

These initiatives normally have "corporate" components as well as "site-level" components. Typically, in larger organizations that are spread across multiple locations and facilities, the organization will focus on pilot sites – perhaps 3-5 – that will represent a range of different types of locations for the "site-level" components. The foundational initiatives will be rolled out at these sites and they will act as "lead dogs" to be ahead of the pack in implementing greater levels of maturity over time
This first phase of execution will likely include several key elements:

- Central components such as policies on sensitive data or password standards, procedures such as management of change or patching, and technology such as a central reporting functionality
- Site-level components such as asset inventory, configuration baselines, and network design/ segmentation reviews
- Establishing key decision points such as which controls will not apply to certain assets, decision-making on risk-reward or cost-benefit trade-offs, and rules for "technical feasibility exceptions" where devices such as PLCs or older HMIs may not be able to meet control standards and will require some form of compensating controls

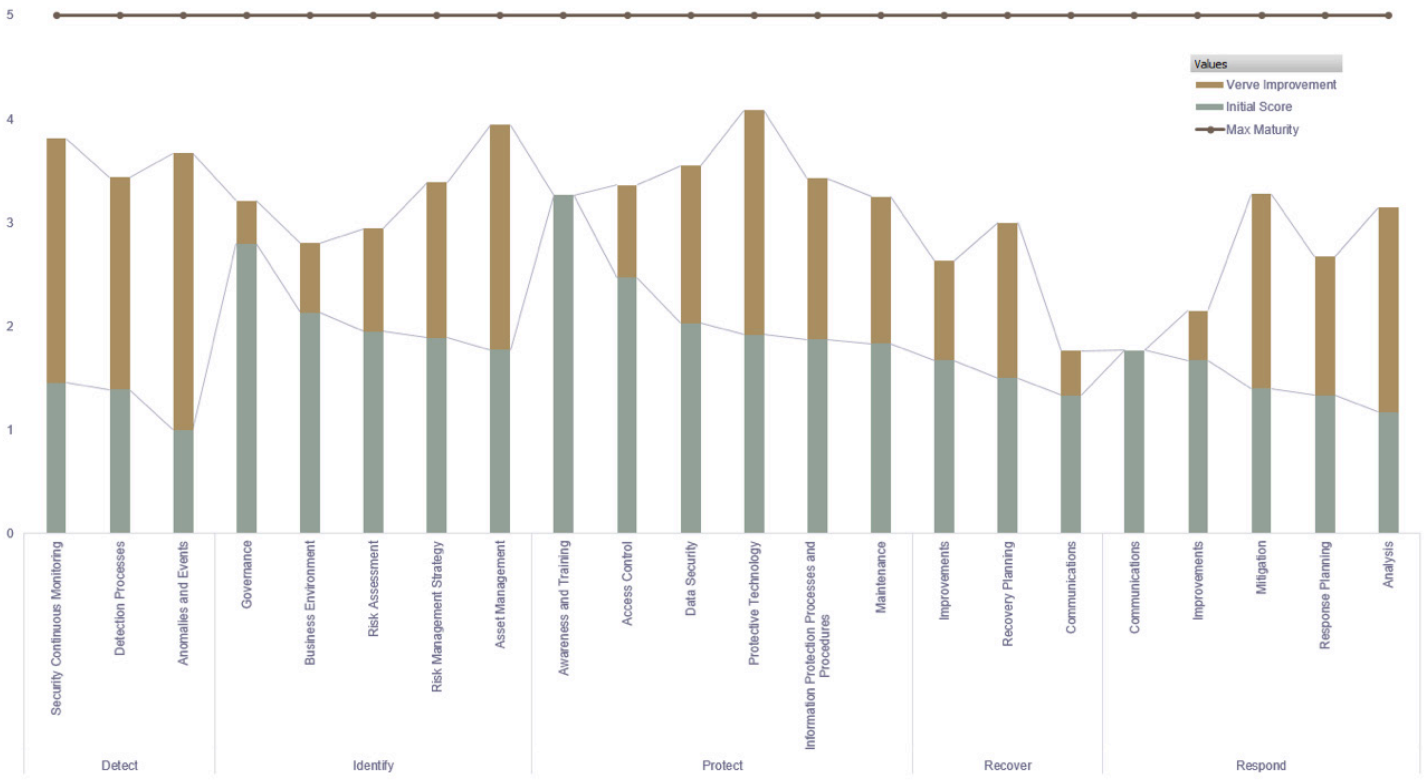
STEP 4 - BUILD ON FOUNDATION

At this stage most organizations are now executing on successive but complimentary additional projects. In most cases this means clients are now rolling out proven tool sets to multiple, additional sites as well as embarking on second or third phase security tool and procedure design, testing and deployment in pursuit of a rich, multi-layered security program. It is at this stage that the effort put into the earlier stages of rapid assessment and Target Maturity Roadmap development really bring significant benefit to a rapid improvement in effective but sustainable security controls and measures.

STEP 5: MONITOR, MEASURE AND IMPROVE

CONTINUOUS FEEDBACK LOOP

SAMPLE SCORE CARD



Critical to the overall program is a robust monitoring & measurement program. Like all things in management, inspection and tracking of progress is critical to improvement. In many cases, companies forget about these measurement and tracking components until they have already done steps 1-4. The resources, tools, and budgets for ongoing monitoring & measurement need to be considered up front. The measurement not only provides a status report, but also enables course correction as the initiatives are executed. The roadmap will certainly evolve over time, and measuring progress and issues as it proceeds is critical to intelligent evolution.

As stated at the beginning, cybersecurity maturity is a journey, not a destination. The key to a successful program will be its ability to continually improve the maturity level over time as new risks are identified and new solutions developed. The roadmap described above should be a living document. The foundational elements and "glue" that integrate the information and tools together should enable the maturity levels to grow over time.