IVT NETWORK
INSTITUTE OF VALIDATION TECHNOLOGY | an informa business
Unlimited Validation Knowledge Awaits...
Published on *IVT Network* (http://www.ivtnetwork.com)

Cybersecurity and CyQ

By **Valarie King-Bailey**

Apr 25, 2018 7:00 am EDT

BACKGROUND

Cybersecurity threats are a clear and present danger that looms over every company no matter what the size. Compromise, destruction or theft of data held within validated systems can inflict significant damage or result in significant non-compliance violations. Validated systems manage mission critical quality and regulatory information required by predicate rules. For years, validation engineers have based their efforts on the principle that validation should provide documented evidence that a system performs according to its intended use. During the validation exercise, confirmation of security controls, 21 CFR Part 11 assessment and testing (if applicable) and qualification testing activities are conducted to ensure the proper installation of computer systems as well as their performance and proper operation. In simpler times, the primary concern centered on the functionality of the application and the aforementioned testing. Cybersecurity readiness was not a part of the equation.

Today's technology advancements are moving at the speed of thought, yet comprehensive regulatory guidance has not kept up with the times.   Guidance for computer systems validation as highlighted in the U.S. FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff - January 11, 2002. The current guidance does not mention mobile applications, the Internet of Things (IoT), cloud computing, or cybersecurity for validated systems. Of course, this guidance was written during a period where technology was emerging and cloud/mobile technologies had not been widely adopted for validated computer systems.

Times have changed. Life sciences companies are adopting cloud and mobile technologies at increasing rates. The responsibilities for computer infrastructure and software are now in many cases outsourced to providers "as-a-service". Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS) bring new dimensions to the validation process. The questions are "How do I maintain the validated state in the cloud?", "how do I validate IaaS, SaaS, and PaaS? "how can I ensure data integrity in the cloud" and "what due diligence do I need when I deploy cloud or service-based systems I believe the most important questions are on protecting validated systems against cyber attacks, on providing global agencies with documented evidence that a company has completed the requisite due diligence regarding cybersecurity. Remember, if it's not documented, it did not happen. Many validation engineers believe that cybersecurity is the perview of the IT department.   I would remind you of what the mission and the goal of validation -- the process of ensuring that technology meets its intended use. Validation engineers must consider cybersecurity threats and how to protect validated systems against potential threats.

To address the challenges facing validation engineers, today's life sciences companies require practical guidance to deal with the myriad of technology challenges including the Internet of Things (IoT), cloud computing, as to practical guidance to deal with the threat of cybersecurity for validated systems. The purpose of this article is to discuss a new strategy for validation and the necessity for change to deal with looming threats posed to validated systems that are potentially cyber attacked.

INTRODUCING CYBERSECURITY QUALIFICATION (CY-Q)

What is Cybersecurity Qualification (CyQ)? What is a CyQ? It is confirmation of a system's protection controls and readiness to prevent a cyber-attack. It is recommended as the new type of qualification for validated systems. All validation engineers should be concerned about cybersecurity given that it is one of the greatest threats and risks to both validated and non-validated systems environments.

NIST CYBER SECURITY FRAMEWORK

The National Institute of Standards and Technology (NIST) introduced a cyber security framework. The five elements of the framework are shown in the figure below.

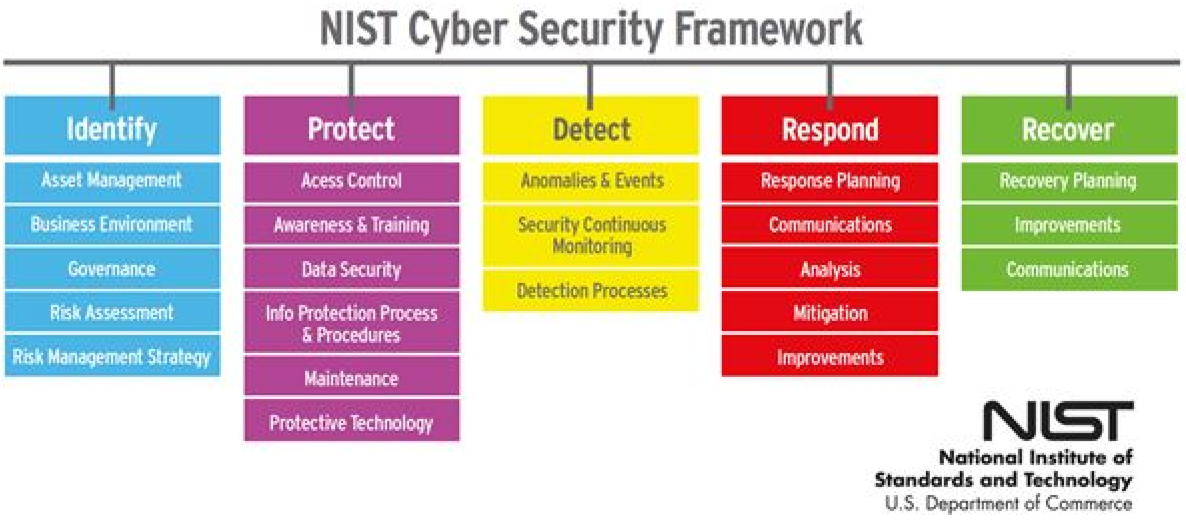


Figure 1 - NIST Cyber Security Framework

The NIST Cybersecurity Framework was created through collaboration between industry and government and consists of standards, guidelines, and practices to promote the protection of critical infrastructure. As validation engineers, our job is to confirm software quality and that systems meet their intended use. How can you realistically do this without paying any attention to the threat of potential cyber-attacks on validated system environment. Use of the Cybersecurity Framework can help validation engineers assess their readiness to protect and defend validated systems. In my practice, we conduct a Cybersecurity Qualification as part of our overall validation strategy. Although not mandated by global regulators, this strategy is common sense. If you stipulate that a system is suitable for production use, it is critically important that you confirm its cyber-readiness. Thus, our full qualification strategy is highlighted below.

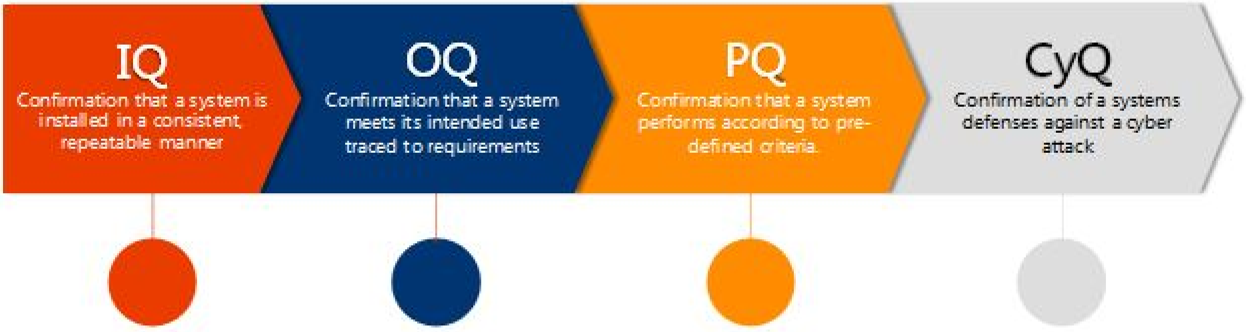
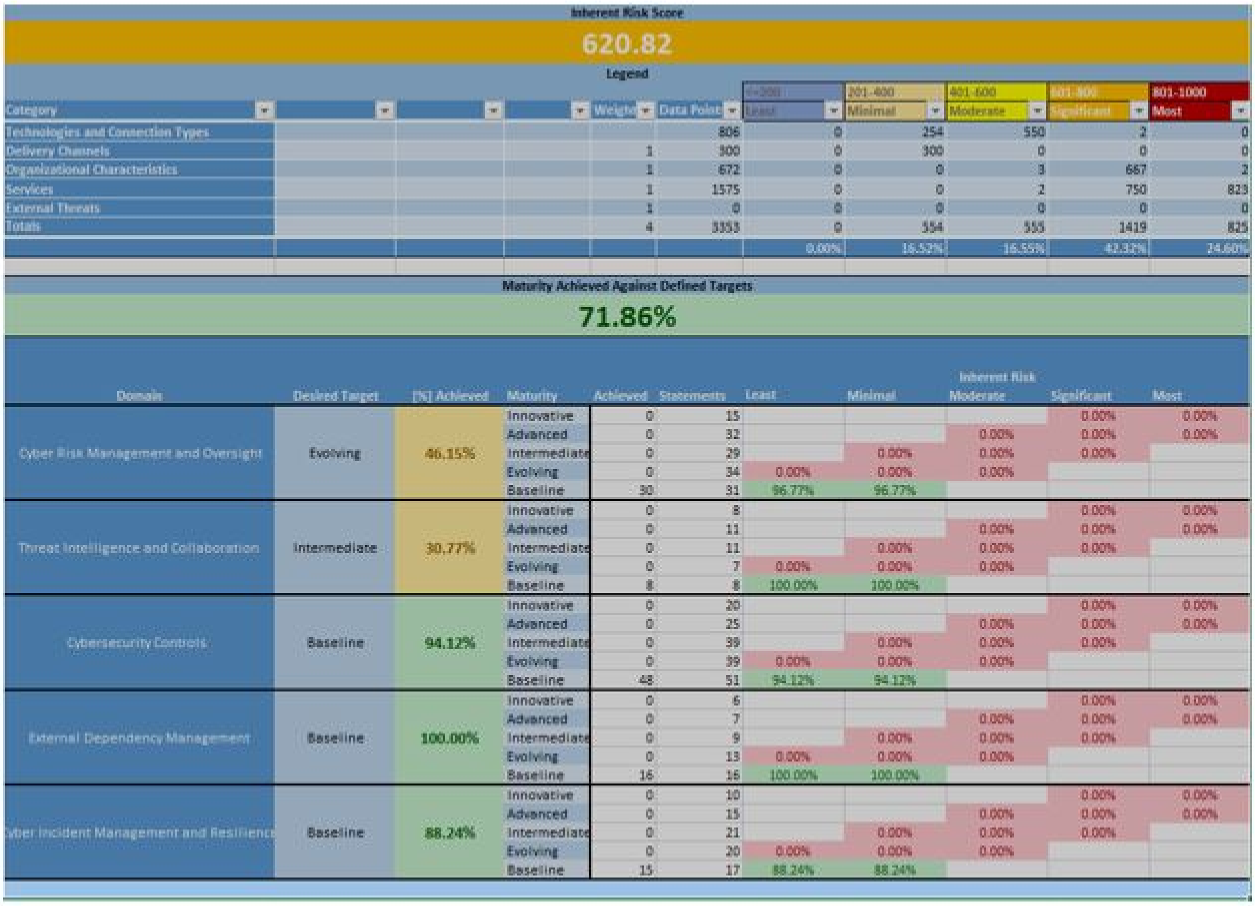

IQ
Confirmation that a system is installed in a consistent, repeatable manner
OQ
Confirmation that a system meets its intended use traced to requirements
PQ
Confirmation that a system performs according to pre-defined criteria.
CyQ
Confirmation of a systems defenses against a cyber attack

Figure 2 - Enhanced Validation Qualification Strategy

CONDUCTING CYQ

So practically, how does one go about conducting a CyQ? We leverage the Cybersecurity Assessment Tool (CAT) developed by the Federal Financial Institutions Examination Council (FFIEC), in conjunction with the National Institute Standards of Technology (NIST). Although developed for financial institutions which have a low risk tolerance when it comes to cybersecurity, the principles are the same for life sciences. The Excel spreadsheet that we use for Cybersecurity Qualification is highlighted in the figure below.



Inherent Risk Score

620.82

Legend

						<=200	201-400	401-600	601-800	801-1000
Category				Weigh	Data Point	Least	Minimal	Moderate	Significant	Most
Technologies and Connection Types					806	0	254	550	2	0
Delivery Channels				1	300	0	300	0	0	0
Organizational Characteristics				1	672	0	0	3	667	2
Services				1	1575	0	0	2	750	823
External Threats				1	0	0	0	0	0	0
Totals				4	3353	0	554	555	1419	825
						0.00%	16.52%	16.55%	42.32%	24.60%

Maturity Achieved Against Defined Targets

71.86%

								Inherent Risk		
Domain	Desired Target	[%] Achieved	Maturity	Achieved	Statements	Least	Minimal	Moderate	Significant	Most
Cyber Risk Management and Oversight	Evolving	46.15%	Innovative	0	15				0.00%	0.00%
			Advanced	0	32			0.00%	0.00%	0.00%
			Intermediate	0	29		0.00%	0.00%	0.00%	
			Evolving	0	34	0.00%	0.00%	0.00%		
			Baseline	30	31	96.77%	96.77%			
Threat Intelligence and Collaboration	Intermediate	30.77%	Innovative	0	8				0.00%	0.00%
			Advanced	0	11			0.00%	0.00%	0.00%
			Intermediate	0	11		0.00%	0.00%	0.00%	
			Evolving	0	7	0.00%	0.00%	0.00%		
			Baseline	8	8	100.00%	100.00%			
Cybersecurity Controls	Baseline	94.12%	Innovative	0	20				0.00%	0.00%
			Advanced	0	25			0.00%	0.00%	0.00%
			Intermediate	0	39		0.00%	0.00%	0.00%	
			Evolving	0	39	0.00%	0.00%	0.00%		
			Baseline	48	51	94.12%	94.12%			
External Dependency Management	Baseline	100.00%	Innovative	0	6				0.00%	0.00%
			Advanced	0	7			0.00%	0.00%	0.00%
			Intermediate	0	9		0.00%	0.00%	0.00%	
			Evolving	0	13	0.00%	0.00%	0.00%		
			Baseline	16	16	100.00%	100.00%			
yber Incident Management and Resilienc	Baseline	88.24%	Innovative	0	10				0.00%	0.00%
			Advanced	0	15			0.00%	0.00%	0.00%
			Intermediate	0	21		0.00%	0.00%	0.00%	
			Evolving	0	20	0.00%	0.00%	0.00%		
			Baseline	15	17	88.24%	88.24%			

Figure 3 -Sample CyQ Assessment

The assessment tool consists of two main sections:

1. **Inherent risk profile:** Identifies the amount of risk posed to a life sciences firm by the types, volume, and complexity of the company's technologies and connections, delivery channels, products and services, organizational characteristics, and external threats — notwithstanding the company's risk-mitigating controls.

2. **Cybersecurity maturity**: (Evaluated in five distinct domains):

a. Cyber Risk Management and Oversight;

b. Threat Intelligence and Collaboration;

c. Cybersecurity Controls;

d. External Dependency Management;

e. Cyber Incident Management and Resilience.

Each domain has five levels of maturity:

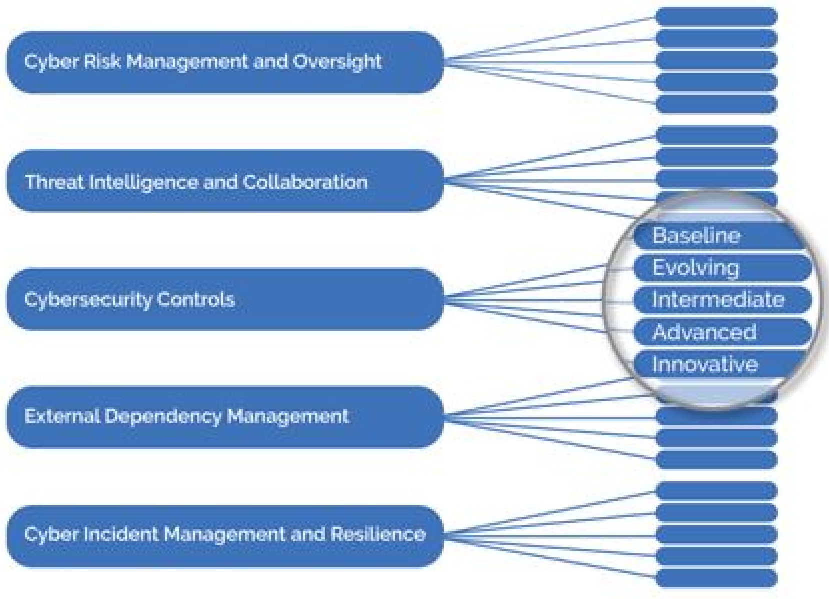

Cyber Risk Management and Oversight
Threat Intelligence and Collaboration
Cybersecurity Controls
External Dependency Management
Cyber Incident Management and Resilience
Baseline
Evolving
Intermediate
Advanced
Innovative

Figure 4 - (5) Levels of Cyber Maturity - Image Courtesy Carbon Black

The CyQ is designed to determine your appropriate cybersecurity maturity level depending on the inherent risk profile. Validated systems should have preventive, corrective, and detective controls to help mitigate against cyberattacks. Preventive security measures include infrastructure management, access and asset management, device/endpoint security, and secure coding practices. Corrective controls may include, but are not limited to, patch management and remediation. Finally, detective controls include activities such as threat and vulnerability detection, anomalous behavior activity detection, and event detection. It is important to provide alerts in real time about both insider and outsider threats would help an organization qualify as Innovative for detective threat and vulnerability measures.

Life sciences companies across the globe are stepping up security efforts in the face of high profile attacks. Some of the lessons learned from recent events are as follows:

- Cyber-attacks are pervasive – no company has immunity
- Attacks may strike validated applications and the associated infrastructure
- Firewalls and anti-malware software are not enough
- Life sciences companies need to understand and assess their level of risk to validated systems
- Defenses for validated systems must be comprehensive
- Cybersecurity assessments and aggressive validation testing/qualification may help identify cyber weaknesses and strategies to mitigate them
- Vulnerability or Penetration Testing alone cannot prevent a breach
- Successful life sciences companies establish a plan and framework to document cybersecurity readiness.

FINAL THOUGHTS

Cyber threats and vulnerabilities can never be fully eliminated and will always be with us. However, life sciences companies can, through comprehensive risk management and cybersecurity qualification (CyQ), understand and mitigate these threats and provide their organizations with a level of confidence that their validated computer systems will be sufficiently resilient to perform according to their intended use.

Source URL: http://www.ivtnetwork.com/article/cybersecurity-and-cyq