Dear NICE:

My input concerning the next version of the NICE framework is attached. I am more than happy to discuss this document further, or provide additional feedback. Thank you for your efforts to improve cybersecurity in the United States.

Best regards,

James

--
James Stanger, PhD
Chief Technology Evangelist
CompTIA
Twitter: @jamesstanger

James Stanger
Chief Technology Evangelist, CompTIA

Twitter: @jamesstanger
Skype: stangernet

13 January, 2020

Subject: Feedback: Input on Updates to NICE Cybersecurity Workforce Framework

To the maintainers of the NICE Cybersecurity Framework:

I am currently the Chief Technology Evangelist at CompTIA, the world's leading tech association. Thank you for the opportunity to provide feedback on the NICE Cybersecurity Workforce Framework. My feedback to your excellent effort is below.

**Social engineering and more sophisticated understanding of communication methods**
Worldwide, the Information Technology (IT) understands that individuals are the primary attack surface. Therefore, it would be wise to include more information about how to improve and manage human "attack surface." Specifically, the revised document should include enhanced awareness of end user training, as well as technical solutions such as endpoint protection and privileged account management (PAM. These practices are very important to many existing job roles.

With the advent of more sophisticated social engineering via media manipulation and Artificial Intelligence (AI), it is also wise to include more information about them. The use of deep fakes, for example, involves more than media manipulation and AI. Handling this issue requires that the NIST document reflect a strong understanding of how attackers take advantage of inadequate communications methods and reporting relationships. It is not enough to protect individuals through training and technical security controls. It is vital to thoroughly investigate and remediate issues where the use of separation of duties and process-based communication breaks down.

**Artificial intelligence**
In the current document, there is virtually nothing specific about:

1. The use of Artificial Intelligence (AI) to conduct attacks.
2. Protecting AI-driven solutions from manipulation.

**Need for enhanced privacy**
The current framework is weak concerning this issue. Government agencies collect exabytes of Personally Identifiable Information (PII). They also obtain metadata from various sources. The revised document should address specific ways to protect PII, over and above traditional job roles and functional skills.

**Enhanced analytics**
The existing analytics section needs to include more information about the use of:

1. Threat intelligence / feeds. This concept is completely absent in the existing document.
2. Threat hunting: Gigabytes of information, some of it even useful, as been written about threat hunting. Whatever term you wish to use, it is important to reflect the cybersecurity industry's interest in moving away from mere threat identification to response.
3. Focused activities: It's impossible to protect 100% of a network. Rather than "boiling the ocean," cybersecurity workers are expected to take a data-driven approach. The NICE document should reflect this current thinking.
4. Threat feeds: If other language is used, then the term "threat feed" should be worked in, as the term is industry-standard.

I recommend that the NICE model update existing job roles and job skills accordingly.

**Enhanced authentication methods: The use of Multifactor and Two-Factor Authentication (2FA) and beyond**

Multifactor Authentication (MFA), which includes Two-Factor Authentication (2FA), is not mentioned by name in the existing document. The document

**Changes in technical support and the help desk / service desk**
The technical support field has continued to morph. The existing NICE document already reflects the passing of the "break fix" help desk professional. Today, there are more technical support and help desk jobs than ever before. The job roles involved in the Information Technology Service Management (ITSM) space have evolved radically.

Today's workers spend more time in the cybersecurity space. In roughly 20% of the companies we work with, we see that help desk / service desk workers do more than just help with login issues and connectivity. Many work hand-in-hand with cybersecurity workers to identify threats and counter them. Technical support individuals are now asked to work with myriad operating systems, drones, and specialized equipment that didn't exist when the existing NICE draft was created.

**Advances in networking**
The NICE document should reflect the use of enhanced network segmentation, including "landing zones" (e.g,. a way to better secure cloud-based connections). I'm not just talking about creating Virtual Private Network (VPN) connections and virtual networks.

Also, the document should reflect the use of SD-WAN, and its uses in security. Finally, edge-based computing is now happening. It is vital to have the NICE document reflect specific changes in existing job roles, as well as new job roles that may be created in the federal space.

**Cloud security**
The government and private sectors have both finally started to actually use cloud-based services. The current NICE document needs to be more cloud-aware. For example, it should:

- Reflect cloud-native penetration testing best practices.
- Include skills focused on analyzing attacks on IoT and serverless architectures.
- Reflect the use of blockchain and other hyperledger technologies, not only in terms of cryptocurrency, but also its use to validate supply chains, create smart contracts, and validate transactions.
- Use Multifactor Authentication (MFA), including Two-Factor Authentication (2FA). I realize that MFA and 2FA aren't limited to cloud implementations. But, it bears repeating.
- Discuss the use of "landing zones."
- Reflect the fact that cloud-based platforms are being used to process massive amounts of information. New job roles now exist that reflect how to create and manage cloud architectures. Existing job roles are also morphing to include new skills and abilities.
- Using cloud services to filter DDoS and other unwelcome traffic.

**Internet of Things (IoT) and Operational Technology (OT)**
At the risk of understanding the issue, the world has stepped up its use of IoT and OT. The document should reflect how existing job roles have morphed accordingly. Issues include:

- Processing OT and IoT data through gateways and edge devices.
- Properly storing data and derived information securely (e.g., data at rest).
- Encrypting data in transit.

The existing document does cover securing data in motion and at rest. But IoT and OT-based traffic has affected job roles and brought in new skills.

**Drones**
Some might maintain that existing verbiage and best practices can be used to describe the secure operation of drones. However, new technical support, cybersecurity, and analytics jobs are now focused around this industry. The revised document should reflect this fact.

**Data analytics and business intelligence**
Data and information is directly related to the IT space. Therefore, more data and information-oriented job roles should be included. These include "technical" IT workers in charge of storage and data warehousing, as non-IT workers such as intelligence analysts and data analysts. Even IT workers are being asked to understand specific skills relating to data analytics. If "information is the new oil," then it's time to remember that IT workers are the ones who effectively own the real estate that stores and transports that information. Additional job roles include business analyst and data specialist.

**Protection against Distributed Denial of Service (DDoS) attacks**
The revised NICE document should include changes in job roles in handling both physical and "logical" DDoS attacks.

The sophistication and frequency of DDoS attacks is increasing almost daily. The conventional approach of simply identifying and responding to traditional SYN floods and botnet-based attacks. Today's workers need to thoroughly understand how to respond to such attacks by using installed solutions (e.g., routers, switches, firewalls, load balancers, alternative ISP connections) and third-party "scrubbers."

**Metrics and their importance to cybersecurity job roles**
In the IT and cybersecurity world, if it isn't measured, it isn't going to happen. Therefore, it is vital for the next NICE document to include the idea of creating real-world metrics, over and above typical Return on Investment (ROI) and tired old Mean Time Between Failures discussions. Metrics should include ideas of how end user training, SIEM tools, and other administrative and logical security controls are improving – or not improving – the security of an organization.

**Additional resources**
CompTIA regularly conducts in-depth research in regards to the IT and cybersecurity space. I welcome you to consult the CompTIA Web site (www.comptia.org), as well as the following resources:

- CompTIA Industry Outlook: https://www.comptia.org/content/research/it-industry-trends-analysis
- CompTIA 2018 Trends in Cybersecurity: https://www.comptia.org/content/research/cybersecurity-trends-research
- CompTIA's Cybersecurity for Digital Operations: https://www.comptia.org/content/research/cybersecurity-for-digital-operations

I am not the only CompTIA employee who works daily with subject matter experts around the United States. If you are interested, I could help assemble a series of panels that would include experts from agencies such as the Department of Health and Human Services, the Department of State, the Pentagon, and various training institutions either run by or affiliated with various branches of the United States military.

I welcome the opportunity to provide additional feedback. Please contact me using any of the information in the header of this document.

Again, thank you for your dedication to improving the cybersecurity of the United States.

Best regards,

James

James Stanger
Chief Technology Evangelist
CompTIA (www.comptia.org)
jstanger@comptia.org