NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Upskilling and Reskilling the Workforce for Cybersecurity Roles

November 14, 2018

National Cybersecurity Career Awareness Week

November 12-17, 2018

Access resources and register how you will participate at:

nist.gov/nice/nccaw

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Upskilling vs. Reskilling

Did “cyber” find you?

- What is the distinction?
- Can higher education bridge the gap? The State of the Cybersecurity Workforce and Higher Education Survey

Certificate or Degree?

Top 5 Reasons

- Job security and demand in the field
- Desire to help and protect, to make a difference
- Interest in the field
- Better pay and the opportunity to make more money
- Desire to learn and continue education

41%

of individuals *would consider returning to college* to earn a certificate or degree to prepare them for a job in cybersecurity

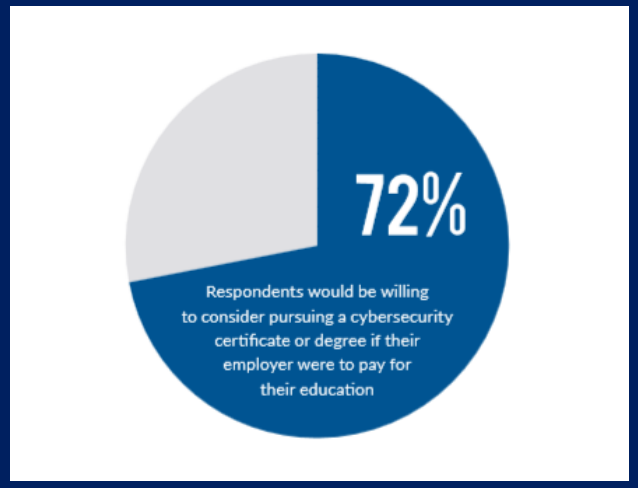
THOSE UNDER THE AGE OF 44

are significantly more *likely to consider getting a degree* to prepare them for a cybersecurity career than those above the age of 45

Partnerships - Employers

Ready Workforce

Findings indicate that employers have a ready and willing pool of potential cybersecurity employees within their existing workforce, if they're willing to spend the time upskilling them and giving them the training they need.



"Those most likely to consider pursuing a cyber education if it were funded by their employer were those between the ages of 35-44"

Partnerships - Government

WIN-WIN

- Diversity and inclusivity
- Quality of and in learning process
- Career-focused professionals

82%
Student retention

3.6
Average GPA

One important observation from my work with federal agencies over the past year is that the more we can work together to find avenues to meet with learning leaders and front-line employees to discuss potential opportunities for development, the more likely we are to see employees remain excited and engaged about their careers in federal service. This is all to say, higher education can be not only a great professional development tool, but also can aid in Federal employee retention efforts.

~Tim Kavanagh, Champlain College Online

Q & A

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Fidelity Investments

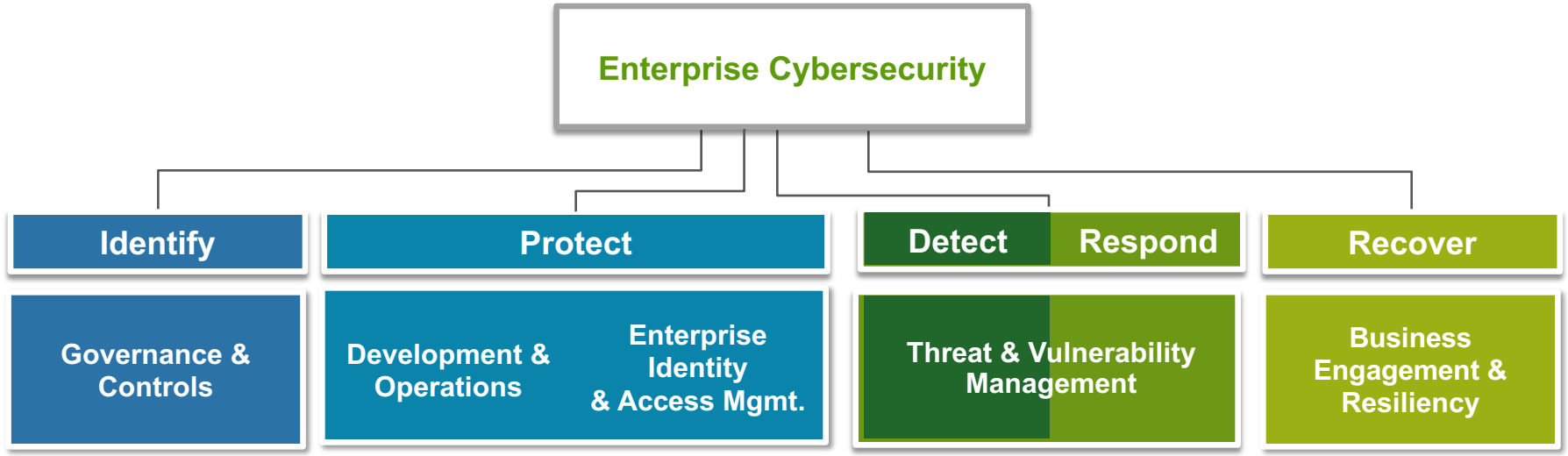
Enterprise Cybersecurity

Chad Johnson

Senior Cybersecurity Consultant

Fidelity INVESTMENTS

Fidelity Investments NIST Framework In Review



NICE Framework Workforce Categories

Fidelity INVESTMENTS

The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

NIST Special Publication 800-181

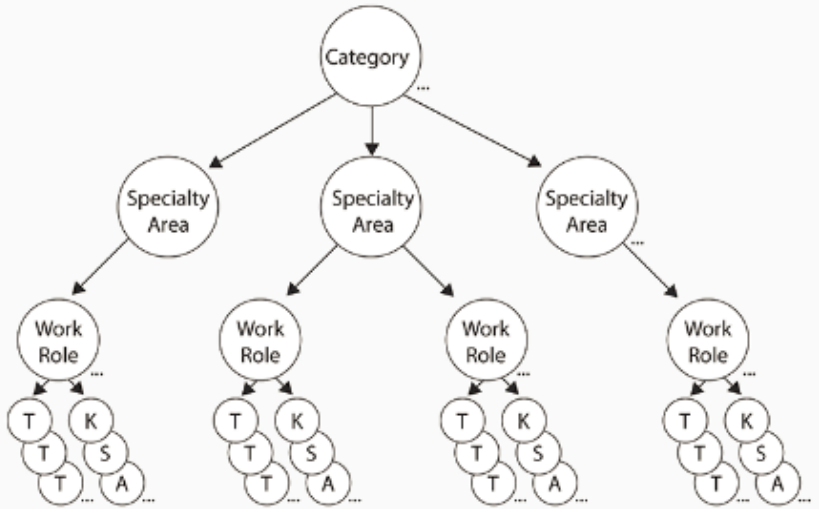
WHAT IS THE CYBERSECURITY WORKFORCE?

A workforce with work roles that have an impact on an organization's ability to protect its data, systems, and operations.

CATEGORIES: A high-level grouping of common cybersecurity functions

SPECIALTY AREAS: Represent an area of concentrated work, or function, within cybersecurity and related work

WORK ROLES: The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role



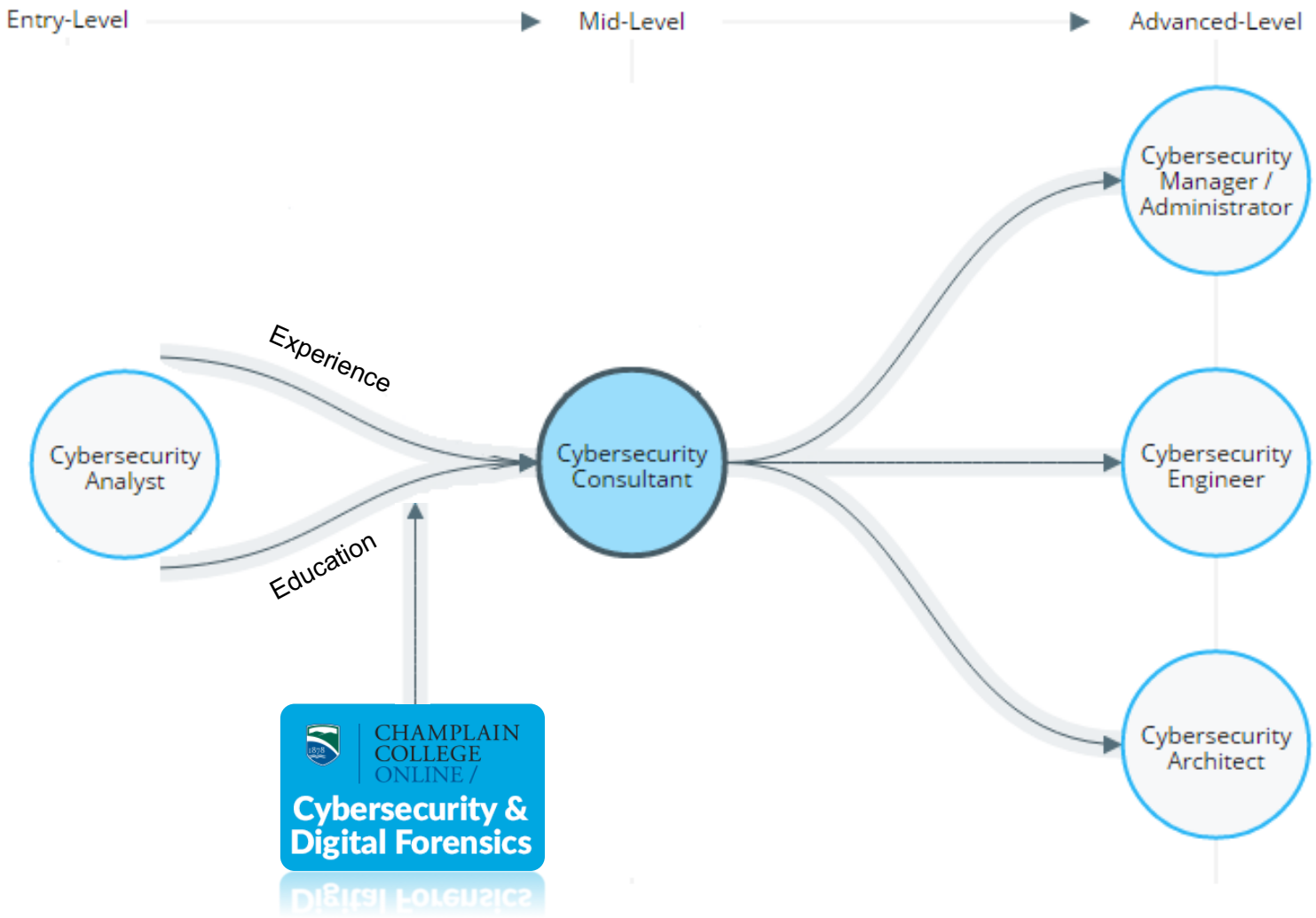
TASKS: Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

KSAs: Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training

NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
CONTACT:
nist.gov/nice/framework
NICEframework@nist.gov

Fidelity INVESTMENTS

Cybersecurity Career Pathway



Fidelity INVESTMENTS

Q & A

Cognizant

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Upskilling and Reskilling the Cybersecurity Workforce

Douglas Meadows

N.A. Delivery Head | Cognizant Security

November 14, 2018

Investment in our People – *"The Reskill Package"*

Upskilling and reskilling is a constant, living and breathing effort within any organizations modern information security program. There are three key-pillars in which we run this effort today within the firm.

Investments Into **Training and Constant Learning**

SANS

CYBRARY

Industry Recognized **Certifications** in Cyber Security

Certifications by leading Security vendors like IBM, Cisco, RSA

Periodic Internal Assessments

ISACA
Trust in, and value from, information systems

(ISC)²

Job Rotation Across Teams and Functions

- ✓ IAM, DPP, GRC, ITM, IVM, Cloud
- ✓ Cloud Security teams with skills across the breath of Cyber Security

Cognizant

Skilling Process @ Cognizant Security

Planning

- Yearly training budget
- Skilling plan based on Demand-Supply of Skills
- Role Development plan based on Full Stack Developer/Engineer path
- Each developer/engineer to carry Fundamental, Adjoining and NextGen skills

Executing

- Dedicated Competency teams to upskill and reskill
- Dedicated Global Capability Dev lead to plan, execute and track skilling efforts
- Certifications to assess skilling
- Quarterly review of skills master table to include upcoming/new demand from markets

Tracking

- Existing Skill Base
- Target vs Actual Skill base reporting
- Training calendar with links for employees
- Reskilled and Upskilled report
- Certifications
- ROI report

Cognizant

Upskilling/Reskilling Snapshot

2018

- **IAM –** Sailpoint, IBM SAM, CA IM, CA SiteMinder, CyberArk, Ping
- **ITM –** CA, Cisco, Symantec, Palo Alto, Qradar, Macfee, Bluecoat, Websense
- **GRC –** RSA Archer, MetricsStream
- **Cloud –** Azure, AWS, Oracle, Google
- **IVM –** Burp, Qualys, Nessus, HPE, Appscan, Checkmarx
- **DPP –** IBM Guardium, CTS Obscure

2019

- IOT Security
- Cloud Security
- **IAM –** Saviynt, JainRain, BioCatch, BehavioSec, Vormetric, Thales, Voltage, PKI
- **ITM -** Imperva, TrendMicro, Zscalar, Logrythm, Tipping Point IDS/IPS, Ayehu, Bit9 Carbon black
- **GRC –** COBIT, SANS, ISO

Real World Information Security Program Examples

"General Medicine i.e. Internal Med or Hospitalist" — *"Sub Specialty - Specialized Medicine – i.e. Dermatology"*

Complexity	General IT Focused Role	Re-Skilled & Upskilled Specialized Cyber Role
★ Reskill	***System or Endpoint Administrator:*** Originally tasked with the management of a domain, user identities and/or antivirus controls.	• **Identity or Access Management** – System admin's or domain administrators are usually neck deep into admin functions that relate to security – good foundation to re-skill. Flipping this to a cyber centric role to manage identity structures, authentication (who you are) and authorization (what you can do) policies can be very straightforward and low barrier of entry into cybersecurity. • **AV / Malicious Code Control Architect** – General IT practitioners who managed endpoints or endpoint controls can easily come into security via the means of managing more hardcore security controls • **Security Configuration Hardening Architect**– Great entry into security via documentation, and configuration standards for technology.
★★ Reskill	***Web Application Developer***	• **Web Application Security :** Very common to see talented / security interested web application developers shift to a web application security architect or governance role given their development background. Developers for the most part are easily groomed to understand tactics around application attacks.
★★ Reskill	***Helpdesk / Tech Support***	• **L1/L2/L3 SOC Analyst:** While automation and SOAR can have an impact on L1 tasks – L1 or even L2 troubleshooting analysts have been seen to make a move into L2 SOC roles due to their analytical skillsets – those same skillsets exerted by good tech support type analysts in IT can be retrofitted into a SOC to focus on commodity malware and reconnaissance type incidents in a SOC. Within large financials and even Cognizant – fusion centers have made this more likely.

Real World Information Security Program Examples

"General Medicine i.e. Internal Med or Hospitalist"

"Sub Specialty - Specialized Medicine – i.e. Dermatology"

Complexity	General IT Focused Role	Re-Skilled & Upskilled Specialized Cyber Role
★★★ Upskill	***Penetration Tester / Forensic Investigator***	• **Threat Hunter:** Threat hunting has become a very common role across many mature information security programs over the past 3 years given the focus on endpoint detection and response (EDR) and automation in the SOC landscape. Upskilling penetration testing consultants or inhouse pen testers to proactively "hunt" in an organization for threats is taking away the traditional detection mindset to a more prevention / early detection activity.
★★★ Upskill	***Data Analyst / Data Scientist***	• **Security Operations and Metrics Analyst :** Data scientists with some training on security tools, tactics, and procedures can be equipped to serve and add value in a SOC in terms of their ability to formulate deep analysis and reporting. • Furthermore, shifting to business risk – they can tremendously add value to the higher level program by deriving and massaging complex data sets from vulnerability management and IRM to provide metrics and security health to executive leadership and the board of directors.

Q & A

Thank You for Joining Us!

Upcoming Webinar:

"Encouraging Cybersecurity Career Discovery via Career Assessment Tools"

When: Wednesday, December 19, 2018 at 2:00pm – 3:00pm EST

Register: https://nist-nice.adobeconnect.com/webinar-dec2018/event/registration.html

nist.gov/nice/webinars

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION