IBM® **Smarter Workforce Institute**

High-Stakes Hiring: Selecting the Right Cybersecurity Talent to Keep Your Organization Safe

Nigel Guenole, Ph.D., Jeff Labrador, Ph.D., Trevor Pons, and Sheri Feinzig, Ph.D.

Cybercrime: A grave economic threat

Cybercrime is pervasive. It exists in every industry. In every country. Every organization is vulnerable to cyberattacks. Estimates of the cost of attacks are eye-watering. In the first half of 2017 there were an estimated 918 data breaches with 1.9 billion records compromised. According to the White House Council of Economic Advisors, the estimated cost of these cyberattacks was between $57 billion and $109 billion.[1] Expert predictions now suggest that an organization will experience a ransomware attack every 14 seconds by 2019.[2]

If these macro-economic estimates are not enough to convince you of the threat of cybersecurity, let's consider specific instances. Verizon reduced its offer for Yahoo's core business by $350 million after a cyberattack compromised more than half a billion user accounts.[3] The latest estimates of the costs of the data breach at Equifax are now over $400 million and let's not forget the impact of cyberattacks on private individuals whose information is compromised by these breaches.[4] In short, cyberattacks are personal, organizational, and financial.

Against this backdrop, it is unsurprising that spending on cybersecurity investments is growing. Worldwide spending on cybersecurity in 2018 is forecast to be $93 billion.[5] The *Wall Street Journal* estimates that by 2022 there will be 1.8 million unfilled cybersecurity jobs.[6] One thing seems certain—spending on cybersecurity protection is growing to meet the increased levels of threat. However, additional spend will only address the threat of cybercrime if it is spent on the appropriate resources to combat the cybersecurity threats.

Elements of a cybersecure organization: technology, process, and people

To secure themselves from cyberattacks, organizations might choose to focus their resources on technology, on process, or on selecting and developing the best people. The strongest approaches to preventing cybersecurity threats will do all three. The technological and procedural requirements for a best practice defense against cyber threats have been covered extensively (see box).

However, regardless of how robust the technical architecture is, organizations must still manage the human side of cybersecurity risks. Selecting the right cybersecurity personnel is of utmost importance. For this reason, effective human resources practices are critical to complement strong technical systems.

More on technological and procedural requirements for a cybersecure organization

Technical guidance for systems engineers and architects is described in the Cyber Insider Prevention report, developed by IBM in association with the Centre for Protection of National Infrastructure.[7] This report is available on request and provides a comprehensive overview of systems controls that organizations can implement to minimize the effects of cyber threats. The controls include information on topics such as information security risk assessments and audits, and network security monitoring.

Cybersecurity personnel risk factors

Cybersecurity personnel can put an organization at risk in three major ways:

1. **Insufficient knowledge.** Workers may not have the technical knowledge to perform their roles in a manner that keeps the organization and its assets secure. An example could be a security analyst not keeping her/his knowledge of industry security protocols current.
2. **Shortcuts.** Workers may take shortcuts in their work, that while benign in intent, leave the organization exposed. An example could be sending sensitive information via email without using appropriate methods such as encryption.
3. **Accidents.** An organization can be at threat from accidents. Here we define an accident as the unintended consequences of independently innocuous but difficult to foresee events that lead to problems when they occur in combination. An example could be when an employee fails to apply the latest security patches and the organization falls victim to a technical vulnerability that experts have already addressed, as purportedly occurred in the recent Wannacry attack on the NHS in the United Kingdom.[8]

Robust hiring procedures can minimize these people risks, but this demands a careful focus on behavioral as well as technical skills.

Hiring beyond technical skills

When it comes to selecting cybersecurity professionals, technical skills are a must, and they can be evaluated by assessment methods such as examining technical credentials, technical interviews, and specially designed simulations. Unfortunately, many organizations are finding it difficult to recruit individuals who have all of the technical skills needed for the job.[9] And, as the *Wall Street Journal* cited earlier made clear, this is a situation that looks set to get worse.

In such challenging circumstances, there is a danger that recruiters and hiring managers are tempted to reduce hiring standards just to get the open positions filled. With such organizationally-critical roles, that could be a very risky approach. However, there is another option and that is to hire beyond just technical skills.

Technical skills are necessary but not sufficient on their own. In fact, our research suggests that the main differentiator between more and less effective cybersecurity professionals is the so-called 'soft skills', not technical skills. It's worth noting that in all of the above security risk situations, it was human error that caused the cost to the business, not technical weakness.

Emphasizing the differentiating nature of behavioral attributes, the *Wall Street Journal* recently reported that, "Employers on the hunt for excellent cybersecurity analysts don't necessarily need to look for candidates with technical skills. More important are the problem-solving skills that you can't learn in a classroom."[10]

"Our research suggests that the main differentiator between more and less effective cybersecurity professionals is the so-called 'soft skills', not technical skills."

Attributes needed for cybersecurity success

IBM industrial-organizational psychologists undertook a research project to identify the essential attributes and aptitudes of high-performing cybersecurity professionals. To do this, they first observed high-performing security analysts (e.g., threat monitoring analysts, incident response and intelligence services analysts, and security information and event management security analysts) in a security operations center. In addition to these observations, these individuals participated in focus groups and surveys to further clarify the requirements. This research revealed several key attributes that distinguished high-performers from average performers.

Four of these identified attributes are summarized in Figure 1.

Figure 1. Sample attributes for cybersecurity success

Resilient Perseveres when faced with intense challenges. Maintains focus when facing unexpected challenges and work obstacles.	**Adaptable** Adjusts to new or changing assignments, processes, and people. Identifies and considers alternative approaches to situations or problems.
Meticulous Utilizes a systematic approach for checking and cross-checking outputs. Accurately gauges the impact and cost of errors, omissions, and oversights.	**Analytical** Uses fact-finding techniques and diagnostic tools to identify problems. Analyzes risks and benefits of alternative approaches and obtains decision on resolution.

These and other identified attributes enable cybersecurity professionals to carry out critical job tasks, such as monitoring security measures, ensuring proper controls are in place, and promoting security awareness throughout the organization.

The benefits of recruiting beyond skills

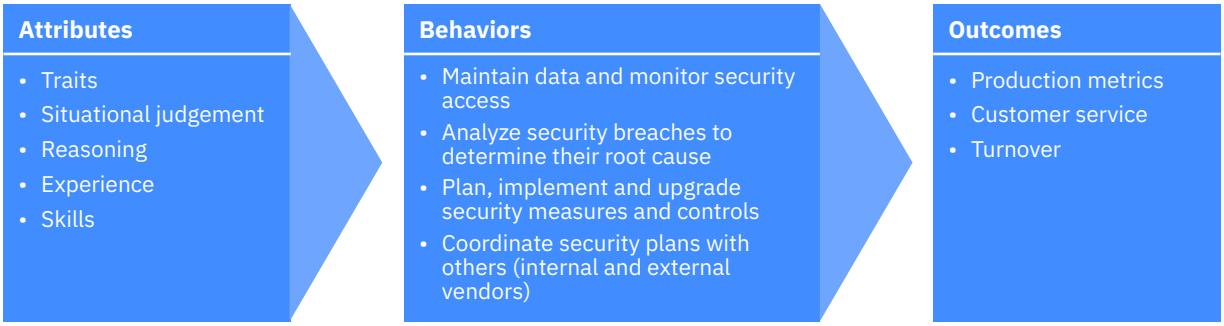
Considering additional attributes beyond technical skills enables recruiters and HR professionals to better address the existing cybersecurity skills gap by:

- **Expanding the talent pool.** Candidates who have not yet acquired all the technical skills needed for the role could also be considered if they have the right behavioral skill set. Once hired, they can be trained in the additional technical skills required.
- **Providing team insights.** A comprehensive list of behavioral competencies provides valuable insights into the strengths and weaknesses of cybersecurity professionals. This information could be used to inform future training and development to improve performance and help employees realize their potential.
- **Selecting the best candidates.** Beneficial behavioral competencies provide important information for talent management tools to identify and select the best candidates for the role. Such selection tools help reduce the costs of a hiring mistake and increase the time to productivity.

What drives people performance?

Technical skills are one element of the full set of attributes that drive job behaviors and contribute to job performance (see Figure 2). Being able to identify the linkage between an attribute, job behavior and performance requires subject matter expert (SME) observation and feedback. One way to fast track this SME work in your organization is to start with the technical and behavioral skills that can be sourced via a comprehensive job and skills taxonomy, such as IBM Watson Talent Frameworks. During a task or job analysis, SMEs will associate the behavior of, for example, 'analyze security breaches to determine root cause' to productivity metrics. In this example, the metrics of interest could be the number of root cause analyses completed, number of tickets closed, and work in progress time. SMEs then identify attributes that are most often associated with the desired behavior. Staying with this same example, our research indicates that the attributes are likely to include analytical thinking, being organized, having a detail orientation, and being adaptable.

Figure 2. Relationships between attributes, behaviors and outcomes



Once these attributes, job behaviors, and outcomes are identified, talent management tools (e.g., assessments, interviews, and recruitment profiles) can be created to aid in finding talent who can demonstrate these key attributes.

What's surprising about cybersecurity professionals?

Jane Wu, Ph.D., Senior Managing Consultant at IBM Talent Management Solutions, conducted a number of the onsite observations in the identification of the critical behaviors for high-performing cybersecurity professionals, including threat monitoring analysts. She explains what was most surprising about this critical organizational role:

"This is not a role where the person can sit in front of a computer and keep to themselves, there is a lot of communication. The communication includes receiving potential cyber issue alerts or concerns from clients. When workers receive those alerts, they not only need to understand what people are describing as a potential risk, they also need to clearly communicate back instructions on what to do. Alongside that, the cybersecurity professional may need to manage the emotions of the person they're talking to.

"The second key feature of cybersecurity work is that it's 24 hours a day and that means shift work. During any shift, there are periods of very high intensity and much quieter periods, so people need to be able to manage their workload effectively. There is also a need to manage the crucial transition between shifts, as employees hand over live issues to co-workers at the end of their working day. This hand-off may not be done in person and that means that the written communication skills of a cyber professional need to be highly developed and effective."

The impact of the right assessment approach to cybersecurity hiring

Using a reliable assessment that considers more than technical skills to identify the right cybersecurity talent enables recruiters to consider a wider talent pool than might otherwise have been the case. This was the approach taken by Julian Meyrick, head of IBM's Security Division in Europe, when he turned to veterans to fill talent gaps in cybersecurity:

"Even though they may not have done the job before, we knew from our cybersecurity assessments that many veterans would be well suited to the roles we had to fill. We saw people with the right competencies for the role, namely high ethical standards, reliability, and a clear understanding that their role is to protect customers. While they need to learn the specific regulation laws and policies and the ability to interpret them, veterans often bring many other soft skills that we find very difficult to interview for. For example, military professionals are proven self-starters, they tend to be motivated, and they take the initiative."

Looking specifically at operators, which includes roles such as threat monitoring analyst, penetration tester, security operations center analyst and cyber operations manager, Meryrick said: *"Anybody who has worked in the operations center in a warship, in a military unit, or in an RAF station is going to have a lot of experience in both dealing with incidents and also training to deal with incidents. I think for me, taking veterans and turning them into cyber operators is typically something relatively easy to do. They frequently have many of the soft skills that are essentially difficult to train people for."*

Learn more about
IBM's Cybersecurity Aptitude Tests →

IBM Smarter Workforce Institute

The IBM Smarter Workforce Institute produces rigorous, global, innovative research spanning a wide range of workforce topics. The Institute's team of experienced researchers applies depth and breadth of content and analytical expertise to generate reports, whitepapers and insights that advance the collective understanding of work and organizations. This paper is part of IBM's ongoing commitment to provide highly credible, leading edge research findings that help organizations realize value through their people. To learn more about IBM Smarter Workforce Institute, visit ibm.biz/Institute

How IBM can help

IBM is a cognitive solutions and cloud platform company that leverages the power of innovation, data, and expertise to improve business and society. By bringing together behavioral science, artificial intelligence, and expert consulting, IBM helps companies attract, hire, and develop the talent they need to grow their business. For more information, visit ibm.com/talent-management

About the authors

Nigel Guenole, Ph.D. is an Executive Consultant with the IBM Smarter Workforce Institute and a Senior Lecturer in Management at Goldsmiths, University of London. He is known for his work in workforce analytics, statistical modeling and psychological measurement. Nigel's work has appeared in leading scientific journals including Industrial Organizational Psychology: Perspectives on Science and Practice and Frontiers in Quantitative Psychology & Measurement, as well as in the popular press. Nigel is also co-author of the book *The Power of People: Learn How Successful Organizations Use Workforce Analytics To Improve Business Performance* (Pearson, 2017).

Sheri Feinzig, Ph.D. is the Director, IBM Talent Management Consulting and Smarter Workforce Institute and has over 20 years' experience in human resources research, organizational change management and business transformation. Sheri has applied her analytical and methodological expertise to many research-based projects on topics such as employee retention, employee experience and engagement, job design and organizational culture. Sheri has presented on numerous occasions at national and international conferences and has co-authored a number of manuscripts, publications and technical reports. Sheri is also co-author of the book *The Power of People: Learn How Successful Organizations Use Workforce Analytics To Improve Business Performance* (Pearson, 2017).

Jeff Labrador, Ph.D. is the Psychometrics and Content Leader for IBM Talent Management Solutions. He has over 10 years of experience designing, validating and implementing large-scale employee selection and development systems. Jeff is a regular contributor to national and international conferences and has co-authored a number of manuscripts, publications and technical reports. His research interests include employee selection, psychological measurement, performance measurement, job analysis, and personality assessment.

Trevor Pons, BSc, BEcon (Hons), M.Econ is a Senior Managing Consultant at IBM. He is a practical Occupational Psychologist focusing on delivering bespoke and client-focused solutions for his customers. He has over 30 years of experience of identifying opportunities for the design and development of new and innovative assessment systems to identify talent and leadership in a wide range of organizational contexts. Trevor has led large teams of design consultants to develop and validate new assessment simulations, exercises, psychometric tests and tools. He utilizes the development of 'task focused' competence models in his assessment solutions and was instrumental in the early development of IBM's Defence Cyber Aptitude Test for UK Ministry of Defence. This solution informed the design and recent release of the CCAT – Commercial Cyber Aptitude Test by IBM.

References

1 White House Council of Economic Advisers (2018) The Cost of Malicious Cyber Activity to the U.S. Economy. Accessed at: https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

2 Cybersecurity Ventures (2017) Cybercrime Damages $6 Trillion By 2021. Accessed at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

3 Roumeliotis, G. & Toonkel, J. (2016) Yahoo under scrutiny after latest hack, Verizon seeks new deal terms. Accessed at: https://www.reuters.com/article/us-yahoo-cyber-idUSKBN14420S

4 Fearn, N. (2018) Equifax: Data breach costs now estimated at $439m as it finds two million more compromised accounts. Computing. Accessed at: https://www.computing.co.uk/ctg/news/3027786/equifax-data-breach-costs-now-estimated-at-usd439m-as-it-finds-two-million-more-compromised-accounts

5 Gartner (2017) Gartner Forecasts Worldwide Security Spending Will Reach $96 Billion in 2018, Up 8 Percent from 2017. Accessed at: https://www.gartner.com/newsroom/id/3836563

6 Nash, K. S. (2017) For Many Companies, a Good Cyber Chief Is Hard to Find. The Wall Street Journal. Accessed at: https://www.wsj.com/articles/for-many-companies-a-good-cyber-chief-is-hard-to-find-1494849600

7 IBM Technical Report Cyber Insider Prevention: Preventing Insider Acts through IT Design. Available on request.

8 Graham, C. (2017) NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. The Telegraph. Accessed at: https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

9 Kennedy, J. (2018) Cybersecurity skills shortage. Accessed at: https://www.csoonline.com/article/3258994/data-protection/cybersecurity-skills-shortage.html

10 Castellanos, S. (2018) Cybersecurity Requires 'Insatiable' Problem-Solving Skills; Technical Skills Can Be Taught. The Wall Street Journal. Accessed at: https://blogs.wsj.com/cio/2018/05/24/cybersecurity-requires-insatiable-problem-solving-skills-technical-skills-can-be-taught/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2018

30018130-USEN-01