RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **HUM-R05V**

Beyond Penetration Testing: Developing a Defensive Cyber-Workforce

Keyaan J Williams

Managing Director
Cyber Leadership and Strategy Solutions, LLC
@_CLASSIlc

Beyond Penetration Testing

Tools and technology help companies achieve the cybersecurity objectives of confidentiality, integrity, and availability; however, you cannot manage security without people.

Beyond Penetration Testing

Finding weaknesses in the environment is important, but there is too much emphasis on offensive red team activities and not enough consideration for the blue team.

Beyond Penetration Testing

The Red Team

- A small number of technical experts working to find holes in corporate defenses.
- Success is measured by finding weaknesses periodically to improve defenses.

The Blue Team

- A larger team of professionals with varying skills who work tirelessly to prevent attacks.
- Success is measured by avoiding failure and everyone gets compromised!

Beyond Penetration Testing

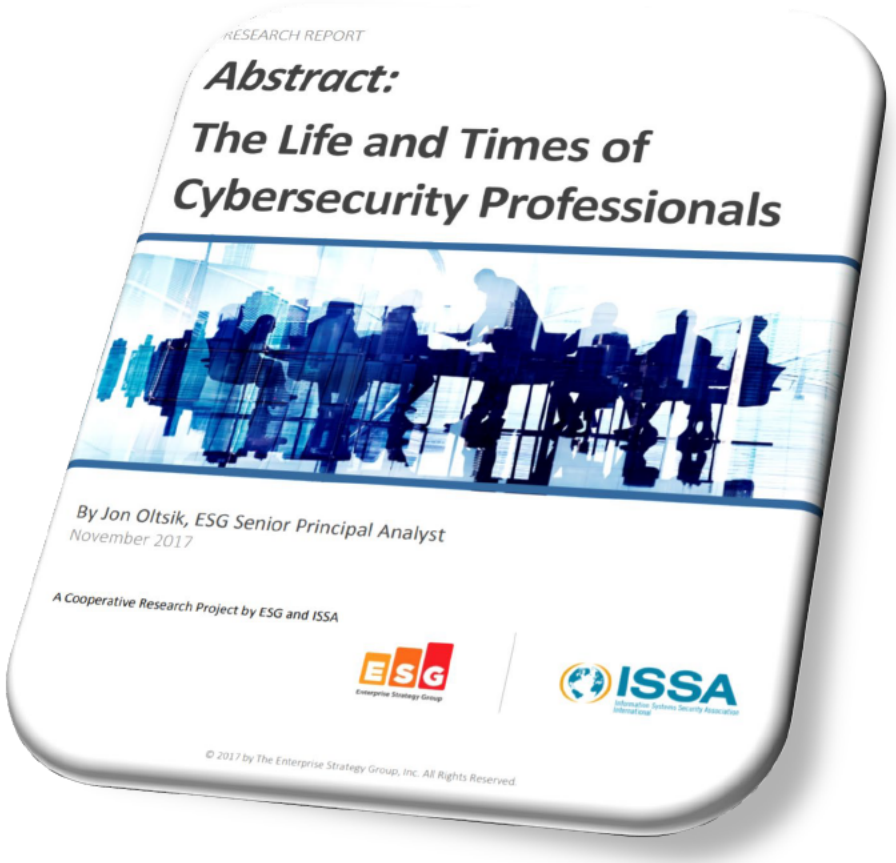
You cannot manage security without people, and you need the right people to be well-trained and ready to support security.

- Findings from the SingHealth data breach highlight the importance of developing people at all levels of the organization.
- A global study from ESG and ISSA confirmed in 2017 “that the cybersecurity skills shortage is exacerbating the number of data breaches.”

Beyond Penetration Testing

Top factors contributing to incidents:

1. A lack of adequate training of nontechnical employees.
2. A lack of adequate cybersecurity staff.



RSAConference2020 APJ
A Virtual Learning Experience

Developing Non-technical Employees

Users are not the weakest link if you prepare them for success

Developing Non-technical Employees

NIST Special Publication 800-50

Building an Information Technology Security Awareness and Training Program

Developing Non-technical Employees

Establishing clear objectives and understanding delivery methods are important concerns for developing non-technical employees.

Security Objectives

- Help employees understand their role in the security program.
- Help employees understand what they need to do.
- Help employees understand why security requires that they doing things a certain way.

Developing Non-technical Employees

Establishing clear objectives and understanding delivery methods are important concerns for developing non-technical employees.

Delivery Methods

- Education
- Training
- Awareness

Developing Non-technical Employees

Investments to develop your non-technical employees increase their ability to support the blue team by identifying anomalies and items of concern in the environment.

RSAConference2020 APJ
A Virtual Learning Experience

Increasing the Adequacy of Your Cybersecurity Staff

Who defends the organization if everyone is focused on penetration testing?

Increasing the Adequacy of Your Cybersecurity Staff

An adequate security team has a balance of offensive and defensive capabilities.

Increasing the Adequacy of Your Cybersecurity Staff

Building defensive capabilities requires the intentional development of a cybersecurity workforce.

- All security people should understand TTPs used in an attack, but this knowledge applies differently for offensive and defensive roles.
- Defenders need a more robust understanding of controls, IT, and communications from the context and perspective of their business impact.

Increasing the Adequacy of Your Cybersecurity Staff

- **Invest in defensive training and certifications.**
- **Test processes and procedures regularly.**
- **Invest in technology and automation that make the defensive job easier.**

RSAConference2020 APJ
A Virtual Learning Experience

Apply

How do you put all of this into practice?

Apply: How do you put all of this into practice?

- Tools are great but you cannot manage security without people.
- Remember that people are people first. They are driven by needs and emotions that have nothing to do with security.
- Remember that all users must understand their role and the contribution they make to the security program.
- Remember to develop a balanced security team. Do not focus exclusively on offensive capabilities.

Apply: How do you put all of this into practice?

NEXT STEPS: Immediate Action

1. Get to know the people in your organization. Don't focus on the board and management. Develop relationships with real stakeholders and users.
2. Develop and understanding about how the business operates and how security influences those operations. How are people using processes and technology to get things done?

Apply: How do you put all of this into practice?

NEXT STEPS: Within three months

1. Establish formal metrics that measure the impact of your efforts to develop the cybersecurity talent in your company.
2. Use the metrics to understand why security issues related to people are getting better, staying the same, or getting worse.
   - Keep it up if things are getting better!
   - Make minor adjustments if things remain stagnant.
   - Make drastic changes in your approach if things are getting worse!

Apply: How do you put all of this into practice?

NEXT STEPS: Long-term Results

1. Successfully developing cybersecurity talent throughout the organization should create a shift in your corporate culture.
   - Continue reinforcing good practices.
   - Continue working to change bad practices.
2. Start working to apply the culture shift to vendors, partners, and external stakeholders. When you get things right internally, you can start to apply these principles to your vendor management program.