

Addressing the **CYBER SKILLS GAP**



The Destructive Nature of Cyberattacks

Cyberattacks are the fastest-growing crimes in the world, increasing in both number and sophistication. Consider these recent attacks:

- The largest-ever Yahoo attack was revised to **3 billion user accounts** affected—up from an earlier estimate of 1 billion—in 2013.
- Marriott suffered the second-largest attack with **500 million user accounts exposed**. Systems supporting Starwood Hotel brands were breached in 2014 and went undetected until 2018—well after Marriott's 2016 acquisition of Starwood.
- Hackers, purportedly from China, penetrated the **U.S. Office of Personnel Management (OPM) in 2012 and went undetected until 2014**. A second group accessed OPM via a third-party contractor in 2014 but was not detected until nearly a year later. Exfiltrated personal data, such as detailed security clearance information and fingerprint data, were stolen.



From data breaches to stolen devices, the results are devastating, costly and can ultimately destroy your customers' reputations.



The Growing Global Need for Cybersecurity

Experts project that global spending on cybersecurity products and services will exceed **\$1 trillion cumulatively** over the five-year period between 2017 and 2021 and overall market growth is expected to be 12-15% per year through 2021.¹

What's more, **cyberattacks will cost the world \$6 trillion annually by 2021.**² These cybercrimes represent “the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.”³



¹ “2019 Official Annual Cybercrime Report,” Cybersecurity Ventures, 2019. ² “2019 Official Annual Cybercrime Report,” Cybersecurity Ventures, 2019.

³ “2019 Official Annual Cybercrime Report,” Cybersecurity Ventures, 2019.



Fighting the Cybersecurity War at a Disadvantage

Waging war against the onslaught of cyberattacks requires the latest technological weapons to detect, prevent and remediate attacks. However, technology alone isn't enough. It also requires battle-ready warriors. According to one expert:

“The greatest virtual threat today is not state sponsored cyberattacks; newfangled clandestine malware; or a hacker culture run amok. The most dangerous looming crisis in information security is instead a severe cybersecurity labor shortage...”⁴

This labor shortage is now close to three million globally, making it the #1 job concern among those who already work in the field—outranking more traditional concerns about lack of budget, time, and work-life balance.⁵

Without a trained cybersecurity army to go up against the growing number of bad guys, it will be next to impossible to bring down the number of cyberattacks.



⁴ “The Equifax and SEC Data Breaches: Takeaways, Reminders & Caveats,” DandODiary.com, 09/28/2017.

⁵ “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens,” (ISC)2, 2018.

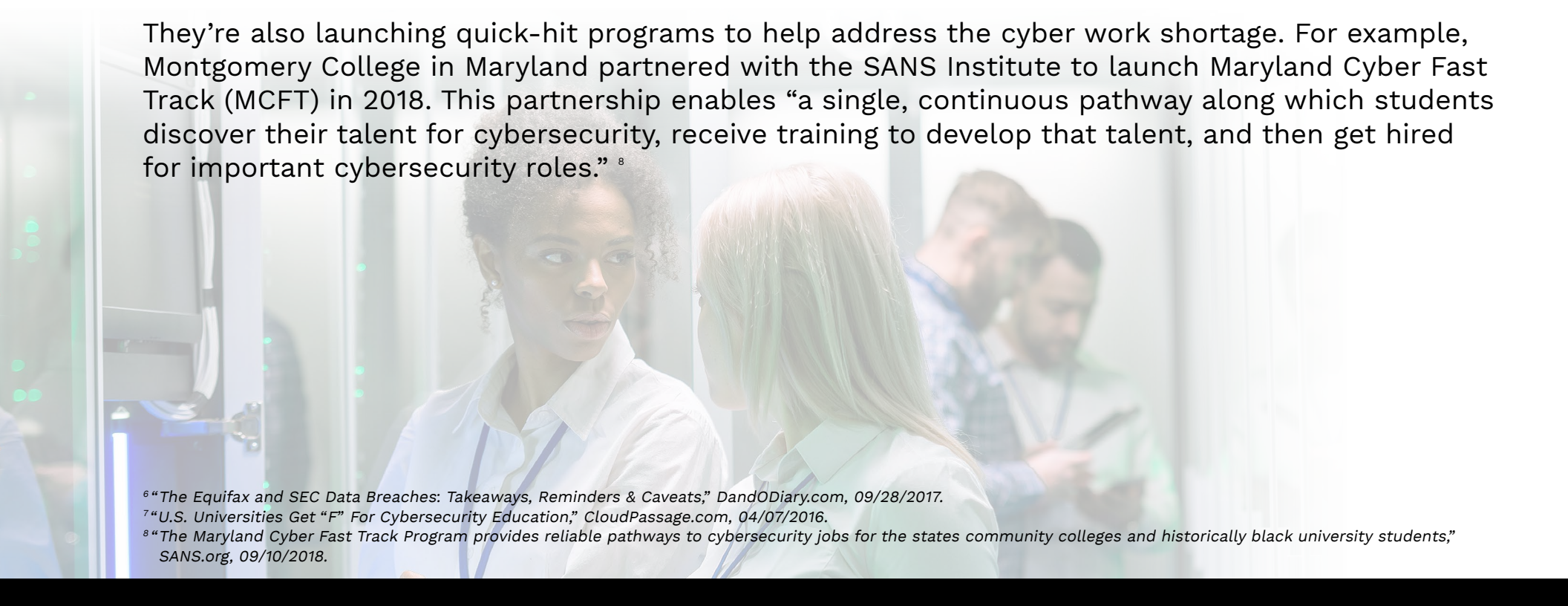


Academia Unable to Keep up With Demand

While the reasons for the shortage of cybersecurity professionals are many, one stands out: “Academia has unfortunately failed to keep up with industry trends and is not producing enough data cybersecurity specialists to handle surging demand.”⁶

In fact, in 2016, none of the top 10 computer science programs in the U.S. required a course in cybersecurity.⁷ Today, more and more colleges and universities have developed—or are developing—four-year cybersecurity degree programs.

They’re also launching quick-hit programs to help address the cyber work shortage. For example, Montgomery College in Maryland partnered with the SANS Institute to launch Maryland Cyber Fast Track (MCFT) in 2018. This partnership enables “a single, continuous pathway along which students discover their talent for cybersecurity, receive training to develop that talent, and then get hired for important cybersecurity roles.”⁸



⁶ “The Equifax and SEC Data Breaches: Takeaways, Reminders & Caveats,” DandODiary.com, 09/28/2017.

⁷ “U.S. Universities Get ‘F’ For Cybersecurity Education,” CloudPassage.com, 04/07/2016.

⁸ “The Maryland Cyber Fast Track Program provides reliable pathways to cybersecurity jobs for the states community colleges and historically black university students,” SANS.org, 09/10/2018.



Hands-On, Real-World Learning Initiatives Matter

Will academic training initiatives be enough though? In a field where the threats are constantly evolving and the means to combat must change with them, traditional educational approaches may be ill-suited to the task.

It may not matter anyway. Surprisingly, “undergraduate and graduate degrees related to cybersecurity matter the least to hiring managers.”⁹ **What does matter? Relevant work experience, knowledge of advanced cybersecurity concepts, and cybersecurity certifications.**

Innovative hands-on and real-world training gained through cybersecurity boot camps, cyber ranges, and cybersecurity certificates can help technology students and professionals become skilled cyber-experts.

For example, tabletop exercises or simulations of the plan in an environment such as a cyber range, can help students—and professional teams—respond faster and potentially contain a breach sooner.

⁹“Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens,” (ISC)2, 2018.

The background of the slide features a blue gradient with a pattern of white padlocks and circuit-like lines. Some padlocks are highlighted with a yellow glow. The bottom of the slide has a faint, abstract graphic of a network or data flow with glowing blue and yellow lines.

What Can You Do to Help Your Customers Address the Latest Threats to Their Businesses?

- **Stay on top of the cybersecurity landscape**—attend relevant conferences, keep certifications current and seek out educational opportunities.
- **Demonstrate your cybersecurity expertise** by uncovering potential threats in your customers' businesses through penetration tests and other related services.
- **Assist customers with professional hands-on training** opportunities at our newly opened Cyber Range.
- **Become a trusted cybersecurity advisor** to your customers.




A Comprehensive Approach to Your Customer's Cybersecurity

Organizations are in dire need of security, which creates incredible growth and earning opportunities for you. Tech Data is committed to pushing the boundaries of NextGen cybersecurity solutions and enabling our channel partners to secure their customers' businesses—from the smallest SMB company to the largest global enterprise.

The Tech Data Cyber Range is the first-ever cyber range hosted by an IT distributor.

By leveraging the Cyber Range, new cybersecurity professionals and seasoned security teams will gain the hands-on skills necessary to design holistic cybersecurity solutions and services that mitigate the latest, most advanced cyber threats.





Tech Data: Helping You Enhance Your Security Practice

As the ever-changing threat landscape continues to evolve—whether in the physical network, cloud, mobility or IoT initiatives—**Tech Data's holistic approach to cybersecurity sets you up for success.** Allow our industry experts, extensive vendor portfolio, and security-related and reseller enablement services, help enhance your security practice.



The top half of the image features a blue background with a pattern of white padlocks and circuit-like lines. Some padlocks are highlighted with a glowing effect. Below this, the text "THANK YOU" is displayed in a large, bold, blue serif font.

THANK YOU

For more information on how Tech Data can help you strengthen your security portfolio, please contact us at securityservices@techdata.com or visit techdata.com/techsolutions/security/.

The bottom half of the image features a light blue background with a pattern of white binary code (0s and 1s) and large, stylized, overlapping geometric shapes that resemble the letters 'A', 'D', and 'T'.