SNAPSHOT

JANUARY 2019

SNAPSHOT 2018

ADDRESSING THE CYBERSECURITY SKILLS GAP THROUGH COOPERATION, EDUCATION AND EMERGING TECHNOLOGIES

> We cannot solve our problems with the same level of thinking that created them.
>
> - Albert Einstein

INTRODUCTION

We live in a period of dramatic change powered by technology. Digital transformation brings enormous economic and social opportunities for people, organizations, and governments. The substantial increase in internet connectivity, the explosion of the number of connected devices, and the rapid up-take of technologies such as cloud computing, advanced robotics, and artificial intelligence (AI) are fundamentally changing people's lives. They are also changing the way organizations do business, and the way governments provide public services and engage with citizens.

At the same time, with every new system or device that is connected to the internet the scope for cyber-attacks grows, as do the consequences of successful attacks. The rise in sheer numbers of attacks alone has been staggering. While difficult to estimate, recent reports show that the number of cybersecurity incidents targeting businesses nearly doubled from the previous year, with more than 159,000 data breaches reportedly driven by ransomware and new attack methods.[1] The financial consequences of a single attack on a single company can reach hundreds of millions,[2] and those estimates do not take into account the broader societal impacts that can result from a significant breach. As cyber-attackers become ever more sophisticated in their operations and cyber-criminals ever more ambitious, we need to collectively find new ways to respond to these challenges.

Neither of these two aspects of digital transformation are new. However, while both public and private organizations may understand the importance of protecting against cybercrime, many of them are not adequately prepared or equipped to face these challenges, sometimes through no fault of their own. As the nature of the threats and the profile of the attackers continue to evolve in scale and sophistication, security teams struggle to keep up in a field where skilled expertise is increasingly scarce. Simply put, the development of critical cybersecurity professionals has been massively outpaced by the growth of the cyber threat landscape – resulting in the cybersecurity skills gap.

The Cybersecurity Tech Accord signatories believe the skills shortage is a priority issue that must be tackled in a variety of ways. This paper, therefore, not only outlines some of the initiatives currently being implemented to close the skills gap. but also looks at the potential of fast emerging technologies, notably Artificial Intelligence (AI), to concretely contribute to a safer cyberspace. Its multi-stakeholder recommendations (education reform, public private partnerships, resetting of businesses' strategic priorities, automation of aspects of cybersecurity, and fostering of AI-friendly policy environments) aim to help policy-makers and business-leaders think through how to mitigate the cybersecurity skill shortage the world now faces.

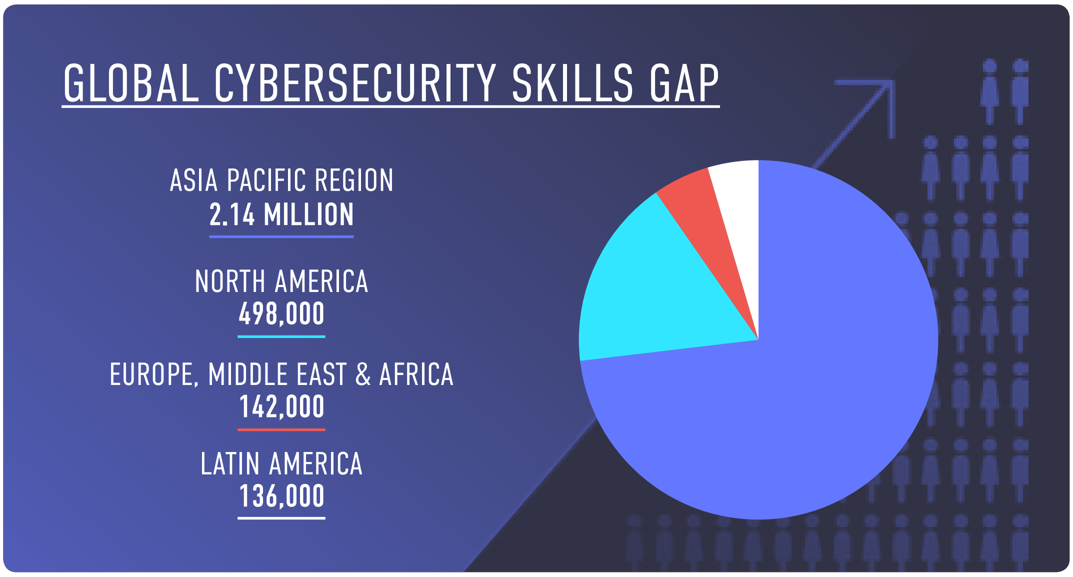
[1] Cyber Incident & Breach Trends Report.   Online Trust Alliance, 2018. https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf

[2] NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs, ZDNet, 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/

THE CYBERSECURITY SKILLS GAP:
THE CHALLENGE WE ARE FACING IS SIGNIFICANT

The last few years have seen a dramatic expansion in the number of people with Internet access. According to the International Telecommunications Union,[3] 55.1% of the world population was online in 2018, which equates to over 3 billion people. Of them, about 2 billion were from developing countries, including 89 million from least developed countries. At the same time, the rise of next generation technologies, such as mobile computing, the Internet of Things (IoT), machine learning, and AI have enabled our societies to become more connected than ever before. This rise in connectivity, of both people and devices, has also made cybercrime more lucrative then ever. Cyberattacks are becoming more sophisticated, growing in frequency and complexity.

This new reality requires our workforce to be sufficiently skilled and agile to cope with these new demands, yet the truth is that we have a clear lack of cybersecurity experts worldwide. A recent study found that 22% of organizations reported that their cybersecurity team is not large enough for the size of their organization, leaving many teams understaffed and burdened with trying to keep up with the escalating volume of cybersecurity challenges.[4] Further research published earlier this year by the International Information System Security Certification Consortium or (ISC)^2 estimates the global cybersecurity skills gap to be just under 3 million people and highlights[5] and the serious real-world impact of this gap around the world. The fast-growing Asia Pacific region is suffering the largest estimated shortfall of 2.14 million cybersecurity professionals, followed by North America (498,000), Europe, Middle East and Africa (142,000) and Latin America (136,000).



[3] Internet World Stats, ITU, 2018. https://www.internetworldstats.com/stats.htm

[4] "The Life and Times of Cybersecurity Professionals" Enterprise Strategy Group (EST), Information Systems Security Association International (ISSA). Nov. 2017. https://www.esg-global.com/hubfs/issa/ESG-ISSA-Research-Report-Abstract-Life-of-Cybersecurity-Professionals-Nov-2017.pdf?hsCtaTracking=a139ebeb-0cf9-4ca1-98ad-d11b1aedc589%7C63333a15-1545-44b2-aece-dccac92fa87c

[5] (ISC)^2 Cybersecurity Workforce Study, 2018. https://www.isc2.org/research

It is clear that a rapid expansion in demand has caught everyone unawares, and unfortunately new cybersecurity professionals cannot be created overnight. Requisite trainings and coursework need to be reflected in our education systems at every level. Dedicated cybersecurity courses were, until very recently, hard to come by, and cybersecurity has often not been made a priority in broader IT training. Additionally, it seems that many high schools and universities have fallen short in promoting IT security as a career path. An Enterprise Security Group study that surveyed 524 millennials and post-millennials in the U.S. revealed that 37% of participants were not interested in the security field simply because they did not know enough about it, while others (28%) cited a lack of technical aptitude.[6] The (ISC)^2 study mentioned above found similar uncertainties in more older respondents as well, who expressed concerns around unclear career paths (34%), and the cost of education to prepare for a career (28%).

The massive worldwide shortage places affected organizations at higher risk of cyber-attack. According to reports, the global annual cost of cybercrime is expected to rise above $2 trillion by 2019. As the skills gap widens, businesses will face a larger exposure to cybercrime and an increased risk to their infrastructure and customers. Organizations seeking to fill positions can experience delays of six to nine months before finding qualified candidates.[7] This dynamic has serious implications, forcing organizations to operate in a critically understaffed environment. As a result, with many IT security teams lacking advanced skills in analytics, forensic investigations and cloud computing, adoption of new technologies is often delayed, leaving organizations to defend their systems with outdated solutions. Furthermore, given the pressure on existing resources, little time is invested in ongoing cybersecurity training, and the job satisfaction of existing cybersecurity staff can be negatively affected.

[6] Millennials Play a Key Role in Solving the Cybersecurity Skills Shortage, Security Intelligence, 2018. **https://securityintelligence.com/news/millennials-play-a-key-role-in-solving-the-cybersecurity-skills-shortage/**

[7] Rise in Cybercrime Continues to Accelerate, Information Age, 2017. **https://www.information-age.com/rise-cyber-crime-continues-accelerate-123467629/**

[8] The Cybersecurity Skills Gap Caused 40% of IT Pros to Stall their Cloud Migrations, Tech Republic, 2018. **https://www.techrepublic.com/article/the-cybersecurity-skills-gap-caused-40-of-it-pros-to-stall-their-cloud-migrations/**

ADDRESSING THE CYBERSECURITY SKILLS SHORTAGE

A growing awareness of the cybersecurity workforce shortage and initiatives launched by the public and private sectors to find solutions represent important step towards making cyberspace more secure. Indeed, today many organizations are actively working to address the current skills gap in different ways. Governments around the world have also made it a priority: in the United States, as outlined in the Office of Personnel Management Guidance released in 2018; with Australian initiatives, such as WithYouWithMe that focuses on retraining skilled military veterans or a $600,000 government grant uniting the University of Sydney and the banking industry to develop a Cybersecurity Challenges for High School program;[10] or the British government's United Kingdom's focus on establishing Academic Centers of Excellence in Cybersecurity Research. [11]

Multi-stakeholder initiatives are also being built and these in particular are likely to be critical to finding enduring solutions. One example is the National Initiative for Cybersecurity Education (NICE),[12] a partnership between government, academia and the private sector, led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce. Since its inception, its mission has been to expand the cybersecurity workforce by accelerating learning and skills development, nurturing a diverse learning community, and guiding career development and workforce planning.

Over the past decade NICE has launched a number of successful initiatives. The NICE Cybersecurity Workforce Framework, developed by NIST and published in August 2017 for example, has been a fantastic attempt to provide further guidance to employers on how to build a capable and ready cybersecurity workforce.[13] The Framework stresses that academic institutions are a critical part of preparing and educating these professionals. It also recognizes that collaboration among public and private entities is what would enable such institutions to determine common knowledge and abilities that are needed in this rapidly evolving sector.

To help shape these forms of collaboration and make them come to life, NICE has funded opportunities to build multi-stakeholder workforce partnerships of employers, schools and institutions of higher education, and other community organizations. These funding opportunities provide assistance to establish Regional Alliances and Multi-stakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development. Through this initiative, NICE has deepened its commitment to closing the cybersecurity [14]skills gap and has had an impact on the supply of skilled workforce also at the local level.

Similarly, companies across the whole spectrum of technology are aware that the demand for qualified professionals represents one of the most consistent security concerns and have taken steps to address this issue, as we will highlight below.

[9] Guidance on addressing the cybersecurity skills gap, OPM, 2018. **https://www.fedscoop.com/cybersecurity-skills-gap-federal-opm-report/**

[10] Australia has just 7% of the cyber security expertise it needs, IT governance, 2018. **https://www.itgovernance.asia/blog/australia-has-just-7-of-the-cyber-security-expertise-it-needs**

[11] Cybersecurity Skills, UK Government Report, 2014. **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf**

[12] NICE, **https://www.nist.gov/itl/applied-cybersecurity/nice**

[13] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework **https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf**

[14] Regional Alliances and Multi-stakeholder Partnerships to Stimulate Workforce Development, 2017. **https://www.nist.gov/nice/regional-alliances-and-multistakeholder-partnerships-stimulate-ramps**

INDUSTRY INITIATIVES
HOW CYBERSECURITY TECH ACCORD SIGNATORIES ADDRESSING THE SKILLS GAP?

The technology sector has launched several initiatives to create, hire and retain cybersecurity talent, to train cybersecurity professionals for the fast-evolving cyber threat landscape, as well as to develop business partnerships to strengthen in-house capabilities. Importantly, the focus of those is not only on traditional audiences, but on ensuring that underrepresented demographics also find a path towards a career in cybersecurity. Examples of these initiatives can be found among the Cybersecurity Tech Accord's signatories and may stimulate additional ideas on the ways to start closing this gap both in the private sector and, more broadly, in the context of education systems across the world.

Cisco has developed many initiatives to address the gender gap in cybersecurity and help women with their career paths in this space. The Women in Cybersecurity Community is a torch of Cisco's efforts to drive gender diversity and carve paths for women to take on cybersecurity careers.[15] The company is also a strong advocate for introducing young people to cybersecurity in the early stages of education. Cisco invests in programs that range from Science, Technology, Engineering & Mathematics (STEM) initiatives in middle and high schools to cutting edge research in institutions of higher education. For twenty years, Cisco's Networking Academy has offered opportunities for IT career education to six million students in more than 180 countries.[16]

Facebook invests in short, medium, and long-term efforts to demonstrate its commitment to the cybersecurity and technology-focused workforce and broader industry. Facebook conducts a Cybersecurity Program, presently at 10 universities. Facebook has also greatly expanded the schools from which it recruits cybersecurity talent, including Historically Black colleges, and Hispanic serving institutions, as well as conferences including WiCys (Women in Cybersecurity), Grace Hopper, Society of Hispanic Professional Engineers, and the National Society of Black Engineers. In 2018, Facebook also launched a 12-week Cybersecurity for Veterans program designed to engage, inspire, and educate veterans towards a career in cybersecurity and beyond. Furthermore, the Facebook University program has been helping since 2013 to increase the success of a diverse and accomplished cybersecurity and technology workforce. Facebook's commitment has resulted in long-term education work with its TechPrep and Engineer in Residence programs, which focus on computer science fundamentals, advanced coding, and engineering training.

[15] No Longer The Only Woman In The Room: Lessons From Cisco's Michele Guel, Forbes, 2017. https://www.forbes.com/sites/georgenehuang/2017/07/24/no-longer-the-only-woman-in-the-room-lessons-from-ciscos-michele-guel/#25d55f3e4528.

[16] Why Cisco for Education? A long history and commitment to education, https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/why-cisco-education.pdf

In 2015, FireEye and HP launched a global alliance to provide customers with advanced threat protection services and incident response capabilities. The alliance brings together teams of analysts with different expertise and combines FireEye's intelligence resources with HP security services. With a combination of more than 5,000 cybersecurity specialists, the two companies' ongoing partnership has offered a new level of cybersecurity expertise to organizations worldwide and helped them close the expertise gaps among their in-house teams.[17]

In 2016 F-Secure launched Cyber Security Base, a massive open online course, which packages the cyber security knowledge and expertise of F-Secure and the University of Helsinki's Department of Computer Science. The series' contents cover a range of topics participants need to understand in entry-level cybersecurity positions, as well as capture the flag-style hacking challenges and other hands-on exercises to help students apply what they learn. The course series has attracted tens of thousands of students from around the world since it was launched, with hundreds of people completing courses and some even earning credits toward university degrees.[18]

In 2018, LinkedIn partnered with the Colorado Workforce Development Council to support the development of career pathways, employing a unique data set that mapped LinkedIn's Economic Graph data to the NICE framework. Through this exercise, the partnership was able to align the knowledge, skills, and abilities as identified by NICE for the cybersecurity talent pool, to the skill-sets of cybersecurity professionals on the LinkedIn platform through aggregated member data.

[17] Close the Talent Gap, Secure the Future. MIT Technology Review. May 23, 2016. https://www.technologyreview.com/s/601537/close-the-talent-gap-secure-the-future/

[18] F-Secure: Cybersecurity Base: https://press.f-secure.com/2018/11/06/popular-cyber-security-mooc-begins-third-year/

Microsoft

Microsoft India and the Data Security Council of India (DSCI) in 2018 launched the CyberShikshaa, a 3-year program to create a robust pool of skilled cybersecurity women professionals in the country. As part of CyberShikshaa, 1000 women from underserved communities will be trained in ten locations across the country and offered employment opportunities. CyberShikshaa is open to women science graduates between the age of 20-27 years. Supported by the Ministry of Information Technology (MeitY)'s Information Security Education & Awareness (ISEA), CyberShikshaa recognizes the need for diverse talent.[19]

TREND MICRO

Trend Micro recognized the growing need for cybersecurity professionals and aimed to help minimize the skills shortage through several initiatives focused in five of its global centers, located in the United States, Canada, Brazil, Czech Republic and Egypt. These centers recruit individuals from both technical and non-technical backgrounds with no specific cybersecurity experience required. After completing the comprehensive training program, the individuals receive job offers to help fill the need for more trained practitioners across the industry. In total, Trend Micro will support the development of more than 2,500 new cybersecurity professionals by 2022.[20]

NORTHWAVE

In response to an increasing number of customers requesting resources for their cybersecurity teams, Northwave developed two approaches for addressing these needs. The first was the launch of a new service to replace or complement existing cybersecurity functions through The Security Office, allowing organizations to effectively outsource cybersecurity needs. The Security Office consists of dedicated cybersecurity professionals who perform risk assessments to identify countermeasures to implement. These measures cover the aspects of business, bytes and behavior. In addition, Northwave has worked with educational institutions in training persons with unique talents and capabilities for careers in cybersecurity that they may not have otherwise considered.[21]

[19] CyberShikshaa : https://news.microsoft.com/en-in/dsci-and-microsoft-roll-out-cybershikshaa/

[20] Trend Micro Nurtures Global Cybersecurity Talent with 2018 Capture the Flag Event, OA Online, 2018. https://www.oaoa.com/news/business/article_e7b19461-93fa-5954-a3e4-8e1537f49d6f.html

[21] The Monastery – First Cyber Security Company with 100% Social Return. Northwave, 2018. https://northwave.nl/the-monastery-eerste-cyber-security-bedrijf-met-100-social-return/

CAN THE USE OF TECHNOLOGY BE PART OF THE SOLUTION?

The speed of both digital transformation and the growth of online threats we face today has exacerbated the challenges related to the cybersecurity skills shortage set out above. Today's online environment means that organizations need to constantly track and correlate millions of external and internal data points across a number of endpoints in an effort to protect their systems. Not only are increasing numbers of people getting online but sensors, location trackers, webcams, smart vending machines, and other types of devices create vast amounts of data that need to be protected. The volume of information alone would be impossible to manage without the support of machines, a reality that doesn't take into account the fact that all too often companies lack the resources to search through a veritable digital haystack of anomalies for the proverbial needle.

MACHINE LEARNING VS. ARTIFICAL INTELLIGENCE
WHAT DO WE MEAN?

ARTIFICIAL INTELLIGENCE

Artifical intelligence is a branch of computer science that aims to endow computers with some degree of human intelligence, such as the capacity to learn, identify patterns or make predictions.

MACHINE LEARNING

Machine Learning is a subset of AI, and it consists of the techniques that enable computers to figure things out from the data and deliver AI applications.

AI and machine learning can help address this challenge and also mitigate the cybersecurity skills gap throughout the entire spectrum of cyber defense activities, from collecting and analyzing data, tracking threats, calculating existing vulnerabilities, and responding to breaches. Examples of how organizations can benefit from utilizing those techniques include:

PREVENTION

The use of AI and machine learning in prevention has been the focus of cybersecurity efforts for some time, with most of the efforts going towards developing systems that can figure out security flaws and develop and deploy solutions in real time. AI and machine learning are particularly valuable in detecting polymorphic malware and in breaking down threat attributes to better stop new and reengineered polymorphic threats.[22] For example, by learning from Internet activity patterns, machine learning and AI can automatically identify attacker infrastructure being staged to launch the next threat.

[22] Machine Learning and Security: Hope or Hype?, Marsh and McLellan, 2018. http://www.mmc.com/insights/publications/2018/sep/machine-learning-and-security-hope-or-hype.html

DETECTION

AI and machine learning can reduce the workload for cybersecurity analysts by helping to prioritize and automate the manual tasks they typically perform, such as searching through log files for signs of compromises. On average, a cybersecurity analyst investigates 10 to 20 high-risk incidents in a day, categorizing only a few as an actual threat.[23] The investigation into each threat can take hours; and this with analysts being able to leverage AI and machine learning to delegate the tedious task of threat research and investigation. Without this ability, cybersecurity professionals would spend a significantly greater amount of time manually combing through alerts with disparate security tools. For example, AI and machine learning can detect behavioral anomalies to find attackers on the inside or logged in with stolen credentials.

RESPONSE

AI and machine learning can also facilitate responses to attacks. For example, traps can be deployed that create a duplicate of the environment to be infiltrated to make attackers believe they are on the intended path and then use the deceit to identify the culprit. AI-enabled response systems can segregate networks dynamically to isolate valuable assets in safe "places" or redirect attackers away from vulnerabilities or valuable data. This can help with efficiency as analysts can focus on investigating high-probability signals rather than spending time finding them.[24]

Machine learning and AI can be powerful tools to take the pressure off overstretched and understaffed cybersecurity teams in organizations, in particular by providing support to cybersecurity experts and allowing them to spend more time on risk management and other important strategic business decisions. In this regard, organizations can best leverage the added value of AI and machine learning by focusing on the following aspects:

- Fully integrating emerging technologies into the wider investment decisions, specifically identifying the staffing roles where these emerging technologies can support faster and smarter human decision-making;

- As these emerging technologies mature, consider their application as constantly evolving and able to make certain "decisions", e.g. automation can be used beyond basic tasks such as threat detection, but also to gather further threats insights and better manage risks, for example by helping organizations categorize attacks based on threat level and propose adapted responses;

- Build a security team that also includes individuals with AI- and automation-era skills such as programming, coding, a basic understanding of the algorithms that govern AI and machine learning functionality.

[23] AI and machine learning boost cyber security efforts, IT Web: Artificial Intelligence, 2018. https://www.itweb.co.za/content/5yONP7EEpGr7XWrb

[24] Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution, Boston Consulting Group, 2018, https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx

Finally, it is also important to remember that the new tools, algorithms and expertise are widely accessible not just to cybersecurity professionals but cyber attackers, who will not refrain from abusing them to make their intrusions more intelligent and faster. The first documented machine learning based cyberattack was detected in India in early 2017, when malware inserted into the network used machine learning to observe user behavior patterns and mimic them, which made it harder for traditional security tools to detect it. We have seen numerous attacks since. By turning to emerging technologies such as AI and machine learning, organizations are therefore not only trying to fill the gaps left by a shortage of cybersecurity talent, but manage the dramatic increases in data and information, as well as navigate the increasingly malicious threat landscape and counter sophisticated attacks by allowing software to fight software.

LEVERAGING CLOUD COMPUTING TO ADDRESS THE CYBERSECURITY SKILLS GAP

Artificial intelligence and machine learning aren't the only technologies that can help with the cybersecurity skills gap. Cloud computing provides numerous cybersecurity advantages as well; two in particular are worth highlighting as they relate to challenges posed by the cybersecurity skills gap.

A better understanding of the threat environment: The large pool of data points can work to the benefit of security, as it allows cloud providers to look for security intelligence across their whole environment. This data can be used by big data security-intelligence systems to discover malware and network intrusion attempts around the globe.

Outsourcing security maintenance: Cloud providers may manage not just datacenter security but also network controls, identity and access controls, and patching. For example, the cloud provider can take care of some tasks that in traditional environments are time-consuming, such as automatically applied patch management, regular vulnerability and system security configuration scanning and privilege management.

[24] The Morning Download, Wall Street Journal, 2017. https://blogs.wsj.com/cio/2017/11/16/the-morning-download-first-ai-powered-cyberattacks-are-detected/

THE USE OF EMERGING TECHNOLOGIES IN FIGHTING CYBERCRIME TODAY

As indicated above, there is great potential in using artificial intelligence and machine learning in the fight against cybercriminals, rogue hackers, and aggressive nation states. In fact, we have already moved beyond the theoretical. Emerging technologies, combined with more traditional cybersecurity techniques, are already being used to build a stronger defense against new generations of cyber threats. A small selection of how the Cybersecurity Tech Accord signatories have been able to leverage innovation in this space are provided below.

ANOMALI™

Anomali's Threat Platform[26] uses machine learning powered prioritization to sift through threat data and elevate the most relevant threats to analysts.
Machine learning also powers other components of the platform leading to smarter detections and automated analysis of threats. These technologies go a long way to help analysts in being more efficient when triaging and addressing threats.

arm

Arm recently partnered with Cybereason, a company whose AI threat hunting machine is able to asses 8 million incidents per second. The ability to recognize suspicious behavior patterns is a powerful tool as cybercriminals exhibit attack characteristics that can be identified and multiplies exponentially cybersecurity experts' ability to monitor their systems and networks.[27]

CONTRAST SECURITY

Contrast Security[28] creates self-protecting software through the automation of application security. The agent-based instrumentation technology enables DevSecOps teams to continuously and accurately assess and fix vulnerabilities and protect applications with real-time monitoring and blocking attacks. Further automation of application security will help alleviate the skills gap and in part shift some of the cybersecurity responsibility to development teams.

eset
ENJOY SAFER TECHNOLOGY™

ESET Enterprise Inspector (EEI)[29] is ESET's Endpoint Detection and Response (EDR) tool. It works by collecting real-time data about ongoing activity on endpoints, which is then matched against a set of rules to automatically detect suspicious activities. The gathered information is processed, aggregated and stored in a searchable form, creating an overview of unusual and suspicious activities.

[26] Anomali: https://www.anomali.com/

[27] Irresistible forces must be met with immovable objects, Cyberearson, 2018. https://www.cybereason.com/blog/arm-iot-security-chips-endpoints-artificial-intelligence

[28] Contrast Security: https://www.contrastsecurity.com/

[29] Can AI Power Future Malware, We Live Security, 2018: https://www.welivesecurity.com/wp-content/uploads/2018/08/Can_AI_Power_Future_Malware.pdf

hp

HP Connection Inspector[30] is an intelligent, embedded security feature that learns what a printer's normal network behavior looks like and then watches for suspect changes. When it detects unusual outbound data, it notifies administrators, shuts down the suspect communications and then forces a self-healing reboot to remove the malware and stop the attack.

JUNIPER NETWORKS

Juniper Networks Sky Advanced Threat Prevention[31] includes the information and identifiers that traditional threat prevention tools use but, in addition, takes advantage of ambiguous structural and behavioral properties of potential malware to determine maliciousness. Traffic is fed to the cloud to ensure that changes required to adapt to the current threat landscape are made centrally, and customers do not have to change out their firewalls.

Microsoft

Microsoft integrated innovative security automation technology into its Windows Defender Advanced Threat[32] solution to get in front of enterprise-level malware attacks. The AI technology helps to solve alert volume challenges by automatically investigating alerts, applying AI to identify whether a threat is real, and determining what action to take, going from remediation in minutes at scale.

panda

Panda Security leverages a combination of solutions and services for their customers to provide visibility of all endpoint activity, control of all running processes, and to reduce the attack surface. This includes device management and control features, EDR and EPP solutions, 100% Classification and Threat Hunting services, all the data gathered by its Collective Intelligence for more than 28 years, and external IOAs and IOCs, all perfectly synchronized.

RSA

RSA Adaptive Authentication[33] allows customers to manage fraud and digital risk across multi-channel environments by leveraging risk-based authentication and machine learning to protect users accessing websites, online portals, mobile browsers and mobile apps. In fact, it offers 95% fraud detection rates with low customer intervention and it is currently being used to protect more than 1.5 billion consumers worldwide.

TREND MICRO

Trend Micro has been working with and investing in AI and machine learning for a decade. Their innovative technology enables Trend Micro to support key capabilities like proactive detection of zero-hour malware samples, reducing users' needs for updates and more intricate protection against a wider range of potential threats.[34]

[30] Hackers and defenders harness design and machine learning, HP Inc, 2018: http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-2519ENW.pdf

[31] Juniper Networks Sky Advanced Threat Prevention: https://www.juniper.net/assets/uk/en/local/pdf/whitepapers/2000649-en.pdf

[32] Windows Defender Advanced Threat Solution: https://www.microsoft.com/en-us/windowsforbusiness/windows-atp

[33] RSA Adaptive Authentication: https://www.rsa.com/en-us/products/fraud-prevention/adaptive-authentication

[34] Trend Micro: https://blog.trendmicro.com/how-artificial-intelligence-and-machine-learning-are-improving-cyber-security/

CONCLUSION AND RECOMMENDATIONS

As the focus on cybersecurity in both public and private organizations increases, there is a growing realization that a knowledgeable, sophisticated workforce is critical to reducing cybersecurity risk. Every employee, from executive leadership to the rank and file, now has cybersecurity responsibilities. However, managing cyber risks and the security of systems and networks also requires dedicated expertise, and as highlighted in this paper, we currently face an acute cybersecurity skills gap, one that is only projected to grow.

This problem cannot be solved immediately; nevertheless, several concrete things can be done to address the cybersecurity skills gap in the mid- to long-term. This paper particularly has set out examples of existing efforts and initiatives to tackle the gap and has also sought to demonstrate the value that new technologies, such as machine learning and AI, can bring in helping organizations more efficiently investigate and remediate large volumes of cyberthreats. Not only can the combination of machines and human intervention improve performance, a wider adoption of AI can ensure that everyone benefits from its transformational potential, ultimately helping to mitigate the shortage of cybersecurity skills.

However, that will not be enough. Therefore, the Cybersecurity Tech Accord signatories urge both policy makers and the industry to:

1

SUPPORT REFORM IN EDUCATION

Give greater priority to STEM curricula and career paths that adequately prepare future generations to work with emerging technologies;

2

ESTABLISH COOPERATION BETWEEN GOVERNMENT, ACADEMIA AND INDUSTRY:

Use public-private partnerships to identify the cybersecurity skills that are particularly needed, and also to determine how these can be addressed, e.g. through dedicated university courses or certified trainings with the private sector;

3

MAKE THE ADOPTION OF EMERGING TECHNOLOGIES A STRATEGIC BUSINESS PRIORITY

Technologies, such as AI and cloud computing can enable a smaller number of IT professionals to centrally manage certain aspects of security, e.g. patch management or administrative privilege access rights;

4

PREPARE FOR AUTOMATION OF CYBERSECURITY SKILLS

In the near future many cybersecurity functions will be automated. As a result, cybersecurity professionals will have to be trained to add value by dealing with more advanced threats and by utilizing complex data science;

5

FOSTER AI-FRIENDLY POLICY ENVIRONMENTS

Support open and fair markets, ensure the free flow of data, create workable privacy, information-sharing and access to data regimes, and promote greater regulatory alignment and common practices/standards across jurisdictions.

The effort to establish a more secure cyberspace will require improvements in many areas, from improvements in technology, to government policy, to industry standards. Creating a cybersecurity workforce that has the capacity and capability to do the job and ensuring that we leverage the tools we already have available to us, will both be key parts of this process.

WWW.CYBERTECHACCORD.ORG