NORWICH UNIVERSITY Online

Norwich University Strategy to Meet Cybersecurity Workforce Challenge

By **Philip Susmann**, President, Norwich University Applied Research Institutes

1st Edition Published January 2019

Abstract

Cyberattacks are becoming more persistent and sophisticated, driven by criminal groups and nation-states with the power and funding to create cyber brigades. As cybersecurity becomes a growing issue across every industry, companies and government agencies need dedicated and expert personnel to manage different aspects of cybersecurity including networks, cloud security risk assessment, compliance, and forensics. As cybersecurity jobs become more specialized, so must education that trains the next-generation of warriors to defend networks. Lack of competency-based cybersecurity programs result in a shortage of qualified cybersecurity personnel with the right cybersecurity capabilities. To prepare students and adult learners to work in real-world situations, Norwich University offers performance-based education programs that combine knowledge, research, policy experience, and hands-on training. Partnering with the Norwich University Applied Research Institute, the University provides a foundation of cybersecurity theory and exposure to different tools, events, and skills in real-world situations to produce cybersecurity experts skilled in tackling the challenges of more complex and frequent cyberattacks.

Norwich University Strategy to Meet Cybersecurity Workforce Challenge

By **Philip Susmann**, President, Norwich University Applied Research Institutes

Cyberattacks are disrupting and even halting critical operations as both public and private sectors rely on technology to communicate, share information, and support business processes. While digitization makes life easier, intellectual property is jeopardized as hackers find ways into corporate and critical infrastructures.

Cyberspace touches nearly every aspect of our lives. "It is a ubiquitous realm interconnecting every aspect of modern society, enabled by broadband networks and wireless signals, existing within local area networks in schools, hospitals and businesses and within massive grids that power most countries."[1]

The Department of Defense doctrine describes cyberspace as a "global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[2] The different platforms and open architecture used by enterprises within cyberspace lend themselves to attacks. "The easier you made it for machines to talk to each other, the easier you made it for something bad to spread among them".[3]

Types of Cyber Attacks

Lawrence K. Gershwin, National Intelligence Office for Science and Technology, outlines the following potential cyber threats and actors that challenge the United States:[4]

- National government threats ranging from propaganda to espionage and serious disruption with loss of life and extensive infrastructure disruption
- Terrorists with less developed computer network capabilities
- Industrial spies and organized crime groups
- Hacktivists that pose a medium-threat; most focused on propaganda
- Hackers posing a negligible threat of long-term, widespread damage to national infrastructure

Cyberattacks Cause Havoc to Operations

The 2017 AT&T Global State of Cybersecurity survey reported that cybersecurity attacks negatively affected nearly 80% of surveyed organizations in the past 12 months of that year.[5] In 2018, a massive data breach to Hotel Group Marriott compromised the personal information records of up to 500 million customers.[6]

The Wall Street Journal reported that Russian hackers looking to gain access to critical American power infrastructures penetrated the electrical grid by targeting subcontractors. Hackers used several methods to infiltrate the grid including planting malware on sites of online publications frequently read by utility engineers to gain access to their computers. Some experts believe two dozen or more utilities were breached.[7]

"Saudi Aramco, one of the biggest and most powerful oil companies on the international scene, suffered one of the worst hack in world history in 2012. In a matter of hours, 35,000 computers were partially wiped out or destroyed. Without a way to be paid, gasoline tank trucks seeking refills had to be turned away. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk".[8]

In addition to individuals and small groups involved in cybercrimes, national states and signification subnational actors are developing skills to promote political motives into the cyberspace using cyberwar tactics.[9] Labeling cybercrime as the greatest threat to every business in the world, Cybersecurity Ventures predicts that cybercrime will cost the world $6 trillion annually by 2021.[10] The Federal Bureau of Investigation also predicts that the number and sophistication of cyberattacks will continue to grow.[11]

Currently, no laws or standards exist in cyberspace to guide enterprises to retaliate, negotiate or mitigate networks, critical infrastructure or financial assets. Business and government leaders must re-evaluate cybersecurity models in their infrastructures as well as along their value chain to better defend against and even anticipate malicious cyber threats. The most-effective cyber defensive operations take a holistic approach that combines people, processes and technology to identify and protect against threats with speed and precision.[12]

The need for new tools and skilled cybersecurity experts becomes a pressing issue to address cybersecurity requirements. As cybersecurity jobs become more specialized, so must education that trains the next-generation of cybersecurity providers to defend networks. Certification programs and seminars are not enough to prepare up-and-coming or even experienced cybersecurity personnel to address cybersecurity threats; nor, are computer science degrees that bundle a couple of cybersecurity courses within the program. A dedicated, competency-based cybersecurity degree that blends knowledge, comprehension, and application as the foundation of education is necessary to produce next-generation cybersecurity experts with the right skills.

Cybersecurity Challenges

Several significant issues add to the challenges in managing cybersecurity today:

1. More sophisticated cyberattacks
2. Shortfall of trained cybersecurity personnel
3. Lack of hands-on cybersecurity education.
4. Lack of executive awareness of cybersecurity issues

1. More Sophisticated Cyberattacks

According to Cisco's 2018 Annual Cybersecurity Report, cyberattacks are more sophisticated, with malware becoming more vicious. Enterprises are faced with everything from network-based ransomware worms to devastating wiper malware.[13]

A global survey released by ISACA (previously known as the Information Systems Audit and Control Association) reveals that six out of every ten cybersecurity managers believe their organizations cannot handle anything other than simple cybersecurity incidents due to a lack of cybersecurity expertise or an adequate management system that provides guiding principles for dealing with cyber threats, or a combination of both.[14] In the past, a networking engineer or programmer might conduct cybersecurity on the side. Today, enterprises need dedicated and expert personnel to manage different aspects of cybersecurity including networks, cloud security risk assessment, compliance, and forensics.

2. Shortfall of Trained Cybersecurity Personnel

A crushing shortage of trained personnel exists in the cybersecurity field, not in just one position, but across all activities. The unavailability of skilled cybersecurity engineers results in companies using inexperienced staff, with hopes of training them on the job. The cyber threat landscape evolved so quickly that existing cybersecurity professionals cannot keep pace with new skills and demands.

In the past, network operators and telecommunication operators served as primary defenders against cyberattacks. However, as networks become more sophisticated, forces must become more specialized in information assurance. Operational planners along with cyber subject matter experts are needed to support IT environments.9

A lack of professionals trained to acquire and examine evidence is causing backlogs of cases at local, state and federal levels. For example, the Payment Card Industry Data Security Standard requires that a qualified investigator conduct an investigation when situations involve credit card data. Delays result due to the unavailability of qualified resources.

With an increased need to secure operations, organizations are finding that cybersecurity positions are difficult to fill, with the talent gap in this field expected to reach 1.8 million by 2022.[15] In its State of Security 2018, ISACA reported that 55% of organizations announced that open cyber positions take at least three months to fill, while 32% said they take six months or more. And, 27% of US companies said they are unable to fill cybersecurity positions at all.[16]

Until now, organizations did not invest significant funds to train IT staff. According to a 2016 Global CEO Outlook by KMG International, 99 percent of surveyed CEOs reported taking action to develop existing or future talent to address cybersecurity risks. Nearly all expect to increase headcount over the next three years.[17] Current employees, recent graduates, veterans, and women are all untapped cybersecurity resources.[18] Companies struggling to find cyber employees should consider cross-training current staff members, particularly those already in IT.

3. Lack of Hands-On Cybersecurity Education

In 2011, the White House noted the need for scientific rigor in cybersecurity, calling for the development of an organized, cohesive scientific foundation that promotes the discovery of laws, hypothesis testing, and capabilities to design and evolve high-assurance systems.[19] Lack of competency-based cybersecurity programs, along with a shortfall of PhD faculty, result in a shortage of qualified cybersecurity personnel in the United States with the right cybersecurity capabilities.

Most cybersecurity programs are based solely on theory. Students gain the core knowledge but not the hands-on training necessary to become competent to address cybersecurity situations. First responders often lack the knowledge or understanding of what to do when arriving on a crime scene. Corporate investigators should understand how to respond to a cybersecurity incident and find the origin of the attack.

Recent graduates from cybersecurity programs often require additional training and education before working on the line. Educational programs that offer a mix of theory and competency-based experiences will bring more qualified cybersecurity experts to the workforce who can immediately work in the field.

4. Lack of Executive Awareness on Cybersecurity Issues

Greater awareness must exist among corporate leadership regarding the impact of cybersecurity on business. According to findings in KPMG 2016 Global CEO Outlook report, changes led by technology, connected consumers and sector convergence will upend current business models, blur lines between industries and demand a new way of business thinking.[17]

In a value chain very inter-connected with other businesses in both hardware and software, cybersecurity must address the risks of working with third parties. Businesses must ensure suppliers are compliant while adding more security into their own networks.

Next Generation of Cybersecurity Educational Programs

While cybersecurity educational programs exist, only a handful are competency-based. To prepare students and adult learners to work in real-world situations, they must receive performance-based education that combines knowledge, research, policy experience, and hands-on training. Norwich University is unique in its exponential learning experience by offering cybersecurity education that:

- Mixes practical experience with theory so students gain true competency in their field of study (MSISA)
- Engages students in real projects in live situations through the Norwich University Applied Research Institute (NUARI)
- Offers a cross section of different competencies including an understanding of how businesses make decisions and how to engage with senior management (MPA, MSISA, MBA)
- Introduces students to a range of sophisticated cybersecurity products (MSISA)
- Are taught by faculty members recognized for their excellence (see credentials below)

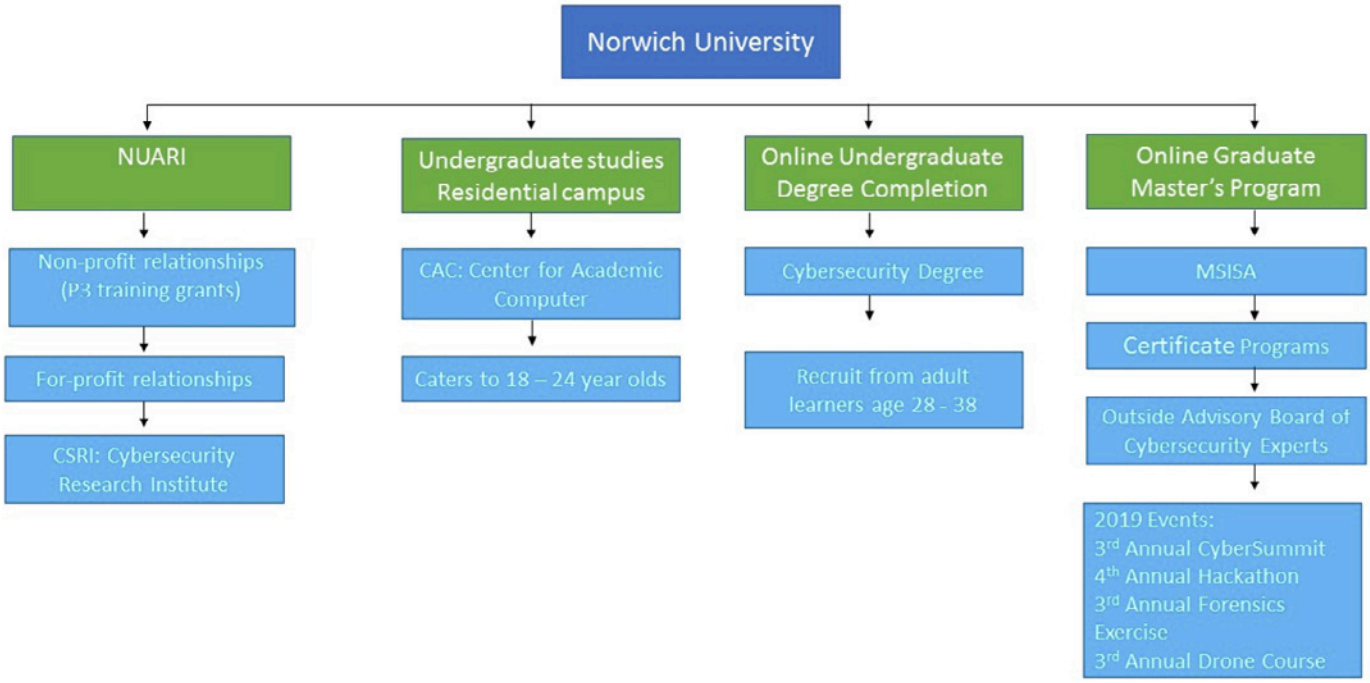
NU Cybersecurity Program Credentials

- Recognized as a National Center of Academic Excellence in Information Assurance Education by the National Security Agency (NSA) and the Department of Homeland Security (DHS)
- Designated as a Center of Digital Forensics Academic Excellence (CDFAE) by the Defense Cyber Crime Center (DC3).
- Member of National Science Foundation's Cyber Corps: Scholarship for Service program.
- Partners with the United States Army Reserves (USAR) to develop cyber-education curricula that align with federal standards and cybersecurity needs.

Many educational institutions offer courses as a component of another degree such as engineering or computing. NU cybersecurity degrees prepare students for Information Security careers in the military, government, industry, and academia. Multi-disciplined academic programs support dynamic education requirements in multiple fields such as forensics and cyber defense. Multi-sector partnerships with the government, industry, academic and military organizations provide opportunities for students to pursue internships, apprenticeships, and full-time employment.

NU offers three distinct learning opportunities in cybersecurity (See Graphic 1) that address the needs of different audiences including students, adult learners and recently discharged military personnel. Participants gain working experience through opportunities provided by the Norwich University Applied Research Institute (NUARI) on a variety of cybersecurity exercises, research programs, and live events.

1. Undergraduate Programs
2. Online Continuing Education
3. Online Master's Degree



Graphic 1: Norwich offers three different learning experiences in cybersecurity that address the needs of recent high school graduates, adult learners and recently discharged military personnel. All are supported by the Norwich University Applied Research Institute that provides opportunities for hands-on training, exercises, and Research & Development.

1. Undergraduate Studies

Norwich University is one of the few schools that offers a Computer Security and Information Assurance (CSIA) degree with majors in Advanced Information Assurance or Digital Forensics. In addition to theory that serves as the foundation for understanding, students can gain hands-on experience working with sophisticated cybersecurity products in real-world situations through Norwich University Applied Research Institute (NUARI). The students also manage a campus cybersecurity computing center and participate in competitions in the Mack Hall war room. NUARI partners with NU in developing CGCS educational activities in cyber security, artificial intelligence, and data analytics.

For example, over 70 CSIA students participated in the Super Bowl 50 cybersecurity event along with NU faculty and local law enforcement authorities. Planning with software vendors and law enforcement over the course of a year prior to the event, students learned about different cybersecurity risks, plans, measures and other activities in a real-world situation. A new group of CSIA students managed cybersecurity at Levi Stadium during the 2019 College National Championship in January, 2019.

2. Online Studies

Designed with working adults in mind, an online Bachelor of Science in Cyber Security combines core principles of cyber security with elective and project-based courses that allow students to explore topics in depth while strengthening skills in critical thinking, communication, and research and analysis. Degrees are customized with a concentration in computer forensics and vulnerability management, or information warfare and security management.

3. Graduate Studies (Cybersecurity)

A Master of Science in Information Security & Assurance (MSISA) program concentrates on information security best practices, organizational structure, and policy development. Students also gain business acumen and management skills to understand complex business enterprises and how to work with teams and management in cybersecurity programs. The MSISA program offers seven concentrations:

1. Computer Forensic Investigation and Incident Response Team Management
2. Critical Infrastructure Protection and Cyber Crime
3. Cyber Law and International Perspectives on Cyberspace
4. Vulnerability Management
5. Project Management
6. Procurement and Government Contract Management
7. Incident Response Team Management and Critical Infrastructure Protection

Hands-on learning experiences are built into curriculum to create greater competency. For example, students concentrating on Computer Forensic Investigation and Incident Response Team Management learn how to manage a cyber-incident response team and react to an incident. Coursework addresses real-life incidents, with skills focused on detection, eradication and recovery. Hands-on labs include forensic imaging, introduction to FTK, network packet analysis and Steganography. In addition, every student, regardless of concentration, is asked to use their companies as an exemplary situation for building a cybersecurity policy based on risk during the course of program.

During a weeklong Capstone residency program prior to graduation, Master Degree candidates participate in real-world experiences related to their majors. For instance, students attaining a Computer Forensic Investigation and Incident Response Team Management degree can conduct investigations with the Vermont State Police, the Northfield Local Police, the Office of the Attorney General and the Vermont Mobile Crime Unit. Those students focused on Vulnerability Management may hack or test various cyber systems for governmental entities or private sector companies.

Master degree candidates such as Jonathan Fitzgerald Lancelot develop white papers on relevant and emerging cyber security topics as part of graduating portfolios. In his cybersecurity paper on "Cyber-Diplomacy and Classical Realism: The Expansion of Anarchy in the Cyber Age", Mr. Lancelot discusses world anarchy over time and the need for universal laws and governs to avoid cyber anarchy.

NUARI Serves Both NU Students and National Public

NUARI serves as the glue that integrates all the educational elements. Created as a separate Research & Development organization to support NU in 2002, NUARI conducts rapid research, education, and training in emerging national security issues. The Institute is comprised of five research institutes:

- Cyber Conflict Research Institute (CCRI)
- Defense Technologies Research Institute (DTRI)
- Institute for Advanced Sciences Convergence (IASC)
- Learning Technologies Research Institute (LTRI)
- International Clean Water Institute (ICWI)

While NUARI offers technical and engineering support to the Department of Defense and works in energy resilience with the Army, its core mission is studying contested information environments to enhance national security, economic security, and national defense to strengthen the U.S. critical infrastructure and secure critical information systems.

Lines of effort include:

- Security operations programs
- Workforce development
- Education
- Technologies development
- Exercises
- Research
- Training

Within these lines of efforts, NUARI often works with NU students conducting on-site research and exercises in developing innovative new cybersecurity programs, tactics, and software that support government and industrial fronts against malicious actors. For example, as part of its security operations program, NUARI built the relationship that facilitated NU student participation in providing cybersecurity during Super Bowl 50 and the 2019 College Football National Championship. The students provided the body of work, deploying technology under the guidance of NU faculty.

Over the years, NUARI supported the NU Engineering Program by bringing critical problems for students to solve as a senior project. For example, one group of students tackled the problem of testing night vision gear for shock testing. Replacing an imprecise testing method that involved swinging a weighted string in a pendulum motion, the electrical/mechanical engineering students developed a pneumatic testing platform that tested the effects of shock while collecting data for reporting. Other projects have included studying the security of digital control systems related to the IoT (Internet of Thing) sensors used as components for monitoring, control, and communications of different assets.

NUARI often engages NU students in different cybersecurity exercises on a national level such as how to respond to cyber events that take place in an interconnected infrastructure. Taking a holistic approach, students evaluate everything from firewall configuration, business risks, and weaponizing ideas. Research projects engage students on relevant cybersecurity topics such as analyzing the time it takes for certain threats to exploit different software. Through this research, students become more familiar with virus structure and how if moves across different systems.

NUARI Presents Diverse Learning Opportunities for Students

In training, NUARI establishes relationships with different government agencies and Fortune 500 companies to gain access to different resources unavailable at most universities on which students can gain learning experience. For example, when working with an external vendor on the Information Warfare side of cybersecurity, NU received a copy of the expensive ROSOKA software used by US Federal Government Intelligence Agencies for analysis of large data sets. NUARI installed the software in a cloud environment to provide access to students to conduct analysis for several different projects.

Through a partnership with Respond Software to integrate its Respond Analyst tool, the first fully autonomous virtual analyst with decision automation, NU students have the unique opportunity to work with this AI software system. The goal of the partnership is to develop student cybersecurity competencies with hands-on experience, as well as to introduce students to next-generation cyber security tools incorporating artificial intelligence and advanced data analytics.

In addition, NUARI helps students obtain internships through multi-sector partnerships with diverse public and private sector stakeholders, a community of governmental and non-governmental organizations, academic and research institutions, and business and industry associations. Typical examples include internships with the State of State of Vermont Security Operations Center conducting penetration testing and West Point participating in research projects. Notable commercial organizations periodically visit the campus interviewing candidates for internships and full-time employment. NUARI works with a range of corporate organizations ranging from HP to SWIFT in placing students in internships.

NU Students Participate in Super Bowl 50 Security

In 2015, over 70 Computer Security and Information Assurance (CSIA) students from Norwich University (NU) worked with law enforcement and homeland security to monitor Super Bowl 50 (SB50) security operations. Invited by the Santa Clara Police Department and the SB50 Critical Infrastructure & Cyber Protection Submission, NU monitored cyber and non-cyber activities leading up to and during the event using the Silobreaker threat intelligence product.

CISA students and NU faculty both on campus and on site at Levi Stadium worked with a collection of public and private security experts tasked with ensuring that spectators, players and local residents remained safe during the Super Bowl. Leading up to the event, CSIA students worked with the lead law enforcement agency to prepare for this globally-televised event and formed partnerships with leading software developers to support the work.

"I was so impressed by these Norwich students and their professionalism, their ability to solve complex problems and the ease with which they have integrated into this intense law enforcement environment," said Captain Phil Cooke, Santa Clara Police Department Super Bowl 50 Commander.

Norwich University CSIA degree candidates provided cybersecurity during Super Bowl 50 at Levi Stadium in Santa Clara, CA. Pictured is (left) NU Professor Huw Reed, Professor, Computer Security and Information Assurance and Director, Center for Advanced Computing and Digital Forensics alongside a recent graduate of the Computer Security and Information Assurance (CSIA) degree program.

Upcoming Learning Opportunities

NUARI is constantly working on new learning opportunities for students. The organization is currently building workforce program and education offerings around the ISAO and State of Vermont Security Operations Center for NU undergraduate and graduate students. More specifically, NUARI intends to work with the State of Vermont in building the first ever Security Situation Center, leveraging the best of human and machine to offer higher value hands-on experience to students who are the future leaders of national cyber defense.

In 2019, Norwich University will participate in the Federal Services Academy Cyber Defense Exercise at Fort Meade. This is the first time a non-service academy will join the competition. Hosted by the National Security Agency and Norwich, participants will include ROTC cadets with plans to commission in the US Armed Services upon graduation.

Other projects include the creation and operation of a research center/program around irregular warfare, cyber warfare and information warfare using the DECIDE software platform in finance, defense, energy, transportation and telecommunications as well as a Norwich DOD Cyber Center in collaboration with participating military schools. Through its participation in the National Cybersecurity Preparedness Consortium, NUARI works on cybersecurity programs with other educational institutions including the University of South Florida, Tampa and University of Texas, San Antonio.

Conclusion

A false sense of security often exists in our nation as companies and individuals believe they are immune to international threats. However, anyone with access to the digital superhighway is at risk to cyberattacks. The threat becomes more persistent, driven not only by criminal groups, but nation-states with the power and funding to create cyber brigades. As the adversaries become more complex and attacks more sophisticated, no one is safe across the ecosystem.

NU recognizes the importance of engaging students in the cybersecurity conversation nationally. As the country experiences a shortage of qualified cybersecurity personnel, NU offers an engaged educational experience to produce cyber warriors equipped with the capabilities to execute higher order activities, threat hunting, risk assessment as well as analytics and synthesis to make organizations safer while operating in a more threat-prone IT environment.

NU, along with NUARI, continues to invest in cyber-based activities to build a stronger education model that engages students in different cybersecurity tactics. With educational programs that provide a foundation on cybersecurity and exposure to different tools, events, and skills in real-world situations, the next generation of cybersecurity experts will be better prepared to face the challenges of more complex and frequent cyberattacks.

References

1. NATO Science for Peace and Security Series D: Information and Communications Security – Vol. 38. Cybersecurity and Resiliency Policy Framework. Edited by Ashok Vaseashta, Philip Susmann, Eric Braman.
2. *The Commander's Handbook on the Law of Naval Operations*. (August 2017). Department of the Navy, Department of Homeland Security, Office of the Chief of Naval Operations, US Marine Corps Headquarters,1-182.
3. Corera, G. (2016). *Cyber Spies: The Secret History of Surveillance, Hacking, and Digital Espionage*. New York, NY: Pegasus Books.
4. Jabbour, Dr. Kamal T. and Devendorf, Dr. Erich. Cyber Threat Characterization. *Cyber Defense Review* Fall 2017, p. 79 – 89.
5. AT&T Cybersecurity Insights. Mind The Gap: Cybersecurity's Big Disconnect. Retrieved at: https://www.business.att.com/cybersecurity/archives/v6/.
6. O'Flaherty, Kate. (2018, November 30). Marriott Breach - What Happened, How Serious Is It and Who Is Impacted? Forbes. Retrieved from: https://www.forbes.com/sites/kateoflahertyuk/2018/11/30/marriott-breach-what-happened-how-serious-is-it-and-who-is-impacted/#4f9901fb7d25.
7. Barry, Rob and Smith, Rebecca. (2019, January 10). America's Electric Grid Has a Vulnerable Back Door – and Russia Walked Through It. Retrieved at: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112
8. Pagliery, J. (2015, August 5). The Inside story of the biggest hack in history. CNN Tech. Retrieved from money.cnn.com/2015/08/05/technology/aramco-hack/index.html.
9. Susmann, Philip, Vaseashta, Ashok, Braman, Eric. Cyber Security – Threat Scenarios, Policy Framework and Cyber Wargames. Norwich University Applied Research Institutes.
10. Cybersecurity Ventures. Cybercrime Damages $6 Trillion by 2021. Retrieved at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.
11. Snow, Gordon, Assistant Director, Cyber Division, Federal Bureau of Investigation. Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington, DC, April 12, 2011. Retrieved at: https://archives.fbi.gov/archives/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.
12. Barrett, Rear Admiral Danella. Cybersecurity: Focusing on Readiness and Resiliency for Mission Assurance. The Cyber Defense Review, Fall 2017, 15-20.
13. Cisco Security Reports. Retrieved at: https://www.cisco.com/c/en/us/products/security/security-reports.html?CCID=cc000160&DTID=esootr000875&OID=anrsc005983.
14. Cybersecurity Nexus. State of Cybersecurity Implications for 2016. Retrieved at: http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf,
15. Tech Republic. The 3 most-demanding cybersecurity jobs of 2017. Retreived at: https://www.techrepublic.com/article/the-3-most-in-demand-cybersecurity-jobs-of-2017/.
16. Tech Republic. 4 tips to help your business recruit, and keep, cybersecurity pros. Retrieved at: https://www.techrepublic.com/article/4-tips-to-help-your-business-recruit-and-keep-cybersecurity-pros/.
17. KPMG. Now or Never. 2016 Global CEO Outlook. Retrieved at: https://images.forbes.com/forbesinsights/StudyPDFs/KPMG-Global_CEO_Outlook-REPORT.pdf.
18. Tech Republic. 5 reasons why you can't hire a cybersecurity professional and what you can do to fit it. Retrieved at: https://www.techrepublic.com/article/5-reasons-your-company-cant-hire-a-cybersecurity-professional-and-what-you-can-do-to-fix-it/.
19. Jabbour, Dr. Kamal T. and Devendorf, Dr. Erich. Cyber Threat Characterization. Cyber Defense Review Fall 2017, p. 79 – 89.

About the Author:

PHIL SUSMANN, President of Norwich University Applied Research Institutes (NUARI)

Phil Susmann has served Norwich for over 35 years as a faculty member, Chief Information Officer, Vice President of Strategic Partnerships and is currently the President of Norwich University Applied Research Institutes (NUARI). NUARI is a research and development activity focused primarily on cybersecurity education and training and cyber war-gaming methodology. NUARI develops innovative software solutions to meet training and education requirements for cybersecurity professionals and institutions. NUARI is the developer of DECIDE-FS, the tool used for the financial services sector cyber exercise series, "Quantum Dawn."

NUARI is associated with Norwich University and its world class cybersecurity education programs at the graduate and undergraduate level, delivered both online and on campus.

Phil completed his undergraduate education at Norwich University and earned an MBA at Clarkson University.