IEEE SA
STANDARDS ASSOCIATION

INDUSTRY CONNECTIONS REPORT



META ISSUES IN CYBERSECURITY

IEEE AND THE PROTECTION OF CYBERSPACE: INCREASING IEEE'S CYBERSECURITY ROLE

Authored by

Greg Adamson

Chair, Meta Issues in Cybersecurity

IEEE

Documents
Document Sharing Hub

Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

ACKNOWLEDGMENTS

The document has been reviewed and updated by IEEE SA's Meta Issues in Cybersecurity Industry Connections activity. "Meta" is used in the sense of "beyond" or "above" the technical details of cybersecurity. The activity was named prior to the use of this term by large data corporation. The multi-disciplinary team is focused on:

- Economics of cybersecurity.
- Psychology/human behavior and cybersecurity.
- Legal aspects of cybersecurity.
- Public policy and cybersecurity.
- Technical aspects of cybersecurity.
- Cybersecurity and policing.
- Cybersecurity and insurance standards.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. 9 November 2023. Printed in the United States of America.

PDF: STDVA26580 979-8-8557-0261-3

IEEE is a registered trademark in the U. S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated. All other trademarks are the property of the respective trademark owners.

IEEE prohibits discrimination, harassment, and bullying. For more information, visit http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html.

No part of this publication may be reproduced in any form, in an electronic retrieval system, or otherwise, without the prior written permission of the publisher.

Find IEEE standards and standards-related product listings at: http://standards.ieee.org.

Copyright © 2023 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association ("IEEE SA") Industry Connections publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied "AS IS" and "WITH ALL FAULTS."

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the ICCom members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

TABLE OF CONTENTS

ABSTRACT 5

1. INTRODUCTION 7
   - 1.1. METHODOLOGY 10
   - 1.2. RECOMMENDATIONS 11
2. FROM WHERE DO VULNERABILITIES COME? 13
3. WHAT IEEE CAN BRING TO CYBERSECURITY 15
   - 3.1. IEEE AS A PLATFORM FOR CYBERSECURITY ACTIVITY 15
   - 3.2. IEEE FELLOWS 16
   - 3.3. MEMBER INTEREST 17
   - 3.4. IEEE GLOBAL CYBERSECURITY STANDARDS 17
   - 3.5. IEEE CYBERSECURITY EDUCATION MATERIAL 20
   - 3.6. TECHNICAL SOCIETIES' CYBERSECURITY ASSETS 20
   - 3.7. IEEE GLOBAL CYBERSECURITY POLICIES 21
4. CURRENT IEEE CYBERSECURITY COMMUNITIES 22
   - 4.1. IEEE ORGANIZATIONAL UNIT STRUCTURES 22
   - 4.2. IEEE SA CYBERSECURITY COMMUNITIES 23
   - 4.3. PUBLICATIONS IN CYBERSECURITY 25
   - 4.4. CONFERENCES AND WORKSHOPS 26
   - 4.5. TECHNICAL SOCIETIES' CYBERSECURITY TECHNICAL COMMITTEES 26
   - 4.6. FUTURE DIRECTIONS INITIATIVES 27
   - 4.7. SOME IEEE WEBSITES AND SOCIAL MEDIA 28
5. EXAMPLES OF EXTERNAL OPPORTUNITIES 28
   - 5.1. CYBERSECURITY INDUSTRY 28
   - 5.2. CYBERSECURITY COMMUNITIES AND SOCIAL MEDIA 31
   - 5.3. TECHNOLOGY COMMUNITIES 32
   - 5.4. STANDARDS DEVELOPING ORGANIZATIONS 34
   - 5.5. GOVERNMENT OPPORTUNITIES 34
   - 5.6. CIVIL SOCIETY INITIATIVES 35
   - 5.7. NONTECHNOLOGY CYBERSECURITY COMMUNITIES 35
6. IEEE SA META ISSUES IN CYBERSECURITY 36
   - 6.1. GENERAL 37
   - 6.1. OVERALL 37

APPENDIX A: INVENTORY OF IEEE CYBERSECURITY ACTIVITIES 40

APPENDIX B: IEEE'S CYBERSECURITY COMMUNITIES 43

APPENDIX C: EXTERNAL COMMUNITIES 48

Documents
Document Sharing Hub

Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

IEEE AND THE PROTECTION OF CYBERSPACE: INCREASING IEEE'S CYBERSECURITY ROLE

ABSTRACT

Cybersecurity Problem

Dependence on technology is growing, particularly since the COVID-19 pandemic. Yet, the safe use of technology depends on cybersecurity, which is failing to keep up. This failure can derail the global benefits that humanity should achieve from cyberspace and its technologies.

Why This Matters

Some four million professionals work in the cybersecurity field. IEEE could play a major role in this global community, and in addressing the growing cybersecurity threat, based on four strengths: IEEE's commitment to advancing technology for humanity; its global presence and independence; its engagement across the technology "stack"; and its experience in both cyber research and industry.

This report reviews the IEEE experience and its potential role in the global cybersecurity community. Feedback is welcome for future improvements and updates to this report.

Recommendations

1. Purpose

Attacks on cybersecurity are attacks on the safety of cyberspace itself and on the benefits that humanity can achieve from this enormous field of technology.

Recommendation 1: IEEE should link dependency on cybersecurity to the achievement of our goal of advancing technology for humanity.

2. Independence

IEEE has members in 160 countries. Most people in the world benefit from their standards every day. IEEE's goal is to promote the beneficial use of technology generally, not narrow national or commercial interests.

Copyright © 2023 IEEE. All rights reserved.

Documents
Document Sharing Hub

Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

Recommendation 2: IEEE should apply its reputation for independence to establishing effective cybersecurity principles and standards.

3. Breadth

Advanced technologies are less predictable, isolated, and mechanical, and more intelligent, distributed, and social. IEEE members are found in all these fields, from power to quantum to societal.

Recommendation 3: IEEE should encourage a broad approach to cybersecurity, not just the obvious vulnerabilities, reflecting the breadth of its members' expertise.

4. Experience

IEEE publishes three of the top four cybersecurity journals, has many standards, conferences, and educational activities, and many thousands of members working in the industry.

Recommendation 4: IEEE should use its areas of deep experience to encourage cybersecurity specialists to make IEEE their professional home.

Documents
Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

1. INTRODUCTION

Cybersecurity[1] attacks are increasingly effective, and traditional assumptions are being overturned. For example, zero-click attacks can place malware on a user device without user action, which is fundamentally different from social engineering traditionally used to plant malware. The COVID-19 pandemic, including work from home (WFH), has significantly increased human dependence on technology in addition to having made organizations accept operational risks so as to enable flexibility of users under remote work scenarios.

In the third decade of the 21st century, cybersecurity is annually less effective, which is directly related to the inability to keep ahead of addressing the rise in hacking (both ethical and unethical). The World Economic Forum (WEF) lists cybersecurity failure as among the highest likelihood risks for the decade.[2] The number of attacks, and the damage that they do, is increasing. IEEE needs to get on the front foot to prepare for attack types that are yet to be developed, and IEEE needs to understand how we are going. Despite government attention and enormous investment, the battle is being lost. The following four examples illustrate this:

- **Ransomware**—A large industry has developed based on weaponized cybersecurity flaws accidentally released by a government agency.[3] This criminal industry is heavily dependent on social engineering, convincing users to activate malicious software such as through email links. Although ransomware has been a significant feature of cybersecurity since 2017,[4] its disruptive potential is becoming greater, not less.[5]
- **Deep Fakes**—While falsified documents such as the antisemitic *Protocols of the Elders of Zion* are a long-standing feature of misinformation, computing processing and artificial intelligence software can now fake voice and video in real time.
- **Zero-Click Attacks**—*Zero-click attacks* download malware to a user's device without user involvement.[6] This breaks the security expectation that a user must click on a link or run an executable

[1] NIST provides two contrasting definitions of cyber-attack, one focusing on the activity to "collect, disrupt, deny, degrade, or destroy information system resources or the information itself," while the other considers the means if the attack, "via cyberspace" (https://csrc.nist.gov/glossary/term/cyber_attack). Both are relevant to this discussion. The cyber field includes both information technology (IT) addressing the digital world and operational technology (OT) addressing the physical or analog world. A technology such as the Internet of Things (IoT) involves both of these worlds. Cybersecurity is derived from cybernetics, an approach to technology spanning digital and analog, and is therefore a term IEEE should promote in discussion of the security challenges in this report (Norbert Wiener, Cybernetics, John Wiley & Sons, 1948).

[2] Emilio Granados Franco et al., "The Global Risks Report 2021" (World Economic Forum, 2021), https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf.

[3] Andrea Peterson, "NSA Hacking Tools Were Leaked Online. Here's What You Need to Know.," *Washington Post*, August 17, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/08/17/nsa-hacking-tools-were-leaked-online-heres-what-you-need-to-know/.

[4] Matthew Field, "WannaCry Cyber Attack Cost the NHS £92m as 19,000 Appointments Cancelled," *The Telegraph*, October 11, 2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

[5] Terry Thompson, "The Colonial Pipeline Ransomware Attack and the SolarWinds Hack Were All but Inevitable – Why National Cyber Defense Is a 'wicked' Problem," The Conversation, accessed December 31, 2021, http://theconversation.com/the-colonial-pipeline-ransomware-attack-and-the-solarwinds-hack-were-all-but-inevitable-why-national-cyber-defense-is-a-wicked-problem-160661.

[6] Ian Beer and Samuel Groß, "Project Zero: A Deep Dive into an NSO Zero-Click IMessage Exploit: Remote Code Execution," *Project Zero* (blog), December 15, 2021, https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html.

Copyright © 2023 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

file to activate malware; they are not dependent on social engineering.

- **Unlimited Security Flaws**—*Zero-day attacks* exploit vulnerabilities against which there is no defense,[7] the digital equivalent of walking through walls. As cyber-physical technology increases, there will be more vulnerabilities, all other things being equal.

While the traditional threats are growing, the dominant cybersecurity framework, the "CIA" triad of confidentiality, integrity, and availability, fails to address cyber-physical challenges of operational technology (OT). The 2010 Stuxnet attack,[8] which destroyed part of Iran's uranium enrichment capacity, illustrates an additional dimension of concern that is now widely discussed in the context of implantable health technologies[9] and critical infrastructure.[10]

Tens of billions of insecure Internet of Things (IoT) devices, the near-universal move to shared cloud services, bring your own device (BYOD), WFH, and the future threat of quantum computing breaking the dependency on public–private key technologies are all contributing to the deterioration of cybersecurity. Technologies such as multifactor authentication (MFA), biometric authentication, formal methods, growing cyber professionals, and zero-knowledge proofs address some vulnerabilities, but new vulnerabilities arise. However, with all the effort devoted to cybersecurity, the adversary appears to have the advantage.

Cybersecurity is not alone as a global challenge today. The threat of climate change, the re-emergence of war in Europe, the continued pandemic, and financial criminality (money laundering and tax evasion) are some of the global threats we are confronting this century. Each has involved challenges for institutions responsible for identifying and addressing them. The cyber threat is unique as it is pervasive; impacts individuals, entities, and countries; and has far-reaching immediate impacts, including threats to lives, identity, and critical infrastructure. However, when we consider threats to cybersecurity that have the potential to derail the global benefits that humanity can achieve from cyberspace and technology in general, it is unclear where the initiative should lie. Nation-states and large corporations are both conflicted and fragmented[11] in their quest for effective cybersecurity. International policy makers and chief executive officers lack the expertise to understand threats

[7] Kaspersky, "What Is a Zero-Day Attack? - Definition and Explanation," www.kaspersky.com.au, June 17, 2021, https://www.kaspersky.com.au/resource-center/definitions/zero-day-exploit.
[8] David Kushner, "The Real Story of Stuxnet," IEEE Spectrum, February 26, 2013, https://spectrum.ieee.org/the-real-story-of-stuxnet.
[9] Health Care Industry Cybersecurity Task Force, "Report on Improving Cybersecurity in the Health Care Industry," June 2017, 96.
[10] Cybersecurity & Infrastructure Security Agency, "National Infrastructure Protection Plan," accessed December 31, 2021, https://www.cisa.gov/national-infrastructure-protection-plan.
[11] L.G. Kun, "Homeland Security: The Possible, Probable, and Perils of Information Technology," *IEEE Engineering in Medicine and Biology Magazine* 21, no. 5 (September 2002): 28–33, https://doi.org/10.1109/MEMB.2002.1044157.

Copyright © 2023 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

in most nations and sectors. Despite its enormous activity, the cybersecurity industry relies on the growing threat to flourish.

Cybersecurity is at a turning point. The COVID-19 pandemic has brought forward several years a global dependence on remote technologies. The professional community now exceeds 4 million.[12] A generation of cybersecurity practitioners who learned their skills elsewhere before coming into the field is being followed by a generation of professionals who have always focused on cybersecurity. Certifications (micro-credentials) predominate in the cybersecurity training field, although a mix of credentials and focused tertiary degrees is more likely in the long-term. Cybersecurity practice among technology providers is poor, threatening many of the expected benefits of their technologies. AI systems are playing havoc with expectations of what is possible and also face a potentially insurmountable lack of training on privacy and ethics. Quantum computing threatens to destroy public–private key cryptography, a key pillar of cybersecurity, at least initially until it can, at scale, provide affordable cryptography that all can implement.

Should IEEE play a significant role in addressing the growing cybersecurity threat? IEEE can bring four unique elements to any field it engages with, and cybersecurity is no exception:

- Its approach to advancing technology for humanity.
- Its global presence and independence rather than a national or commercial alignment when promoting beneficial adoption of technology.
- Its engagement across the whole of the advanced technology "stack," from physical materials through to computer applications and their consequences. Cybersecurity is a cyber-physical phenomenon: it is not possible to secure information independently of the physical world. IEEE professionals work across the cyber-physical boundary, for example, in the critical cybersecurity area of the IoT.
- Its global reach into virtually every center of technology in the world. In addition to these unique characteristics, IEEE standards in the IEEE 802® series provide examples of establishing best practices for the world's technology users in their daily experience. Not addressing cybersecurity could impact IEEE's advancing commitments.

This research identifies two previous attempts to prioritize cybersecurity: the 2014–18 Future Directions Initiative, IEEE Cybersecurity,[13] and a 2017 three-day workshop "Artificial Intelligence and Machine Learning

[12] https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[13] https://cybersecurity.ieee.org/

Documents
Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

Applied to Cybersecurity"[14] seeking to generalize the DARPA Cyber Grand Challenge completed the previous year.[15] Can we learn from these and achieve a high-profile role for IEEE within the global cybersecurity field?

Cybersecurity threats are widely recognized; however, instead of improved approaches, point solutions are promoted. This report addresses the question, "Can IEEE play a significant role in reversing the deteriorating state of cybersecurity?" The structure is as follows:

- Section 2 begins by examining the source and diversity of cybersecurity vulnerabilities as an introduction to the challenges that IEEE could help address.
- Section 3 looks at the strengths that IEEE brings to the field of cybersecurity. These include both features that relate to all of its activities and features specifically related to cybersecurity, the first requirement of the report. Supporting data for this are found in Appendix A.
- Section 4 considers the structures of IEEE, which could contribute to a leadership role in cybersecurity, and includes a summary of current key volunteer activities, focusing on the second requirement of the report. Supporting data for this is found in Appendix B.
- Section 5 looks beyond IEEE at the current global cybersecurity environment, examines a range of actors and their displayed level of interest in improving cybersecurity, and identifies a selection of organizations and individuals who have worked with IEEE on cybersecurity challenges or whose interests are closely aligned. This provides the third requirement of the report. Supporting data for this are found in Appendix C.

1.1. METHODOLOGY

The research for this report drew on the following resources:

- The IEEE cybersecurity asset inventory was primarily undertaken from online resources available through IEEE OU websites, the Member and Geographic Activities (MGA) member interest report, and a listing of standards activities and an extract of IEEEXplore contributions for the previous 12 months.
- The lists of activities and volunteers were developed using a collaborative and iterative method, with input from around 30 IEEE volunteers and staff.

[14] IEEE, "Artificial Intelligence and Machine Learning Applied to Cybersecurity," October 6, 2017, https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/industry/ieee_confluence_report.pdf.
[15] Dustin Fraze, "Cyber Grand Challenge," accessed January 1, 2022, https://www.darpa.mil/program/cyber-grand-challenge.

Copyright © 2023 IEEE. All rights reserved.
Documents Document Sharing Hub
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

- The description of cybersecurity threats was drawn from current literature, including FIRST Common Vulnerability Scoring System (CVSS)[16] and OWASP Top Ten reports,[17] and unstructured discussions with cybersecurity practitioners.
- The list of possible points of engagement outside of IEEE is indicative. Rather than attempting to identify all opportunities, it provides some examples where IEEE is currently collaborating and or that could be reasonably developed.

The document was reviewed and updated by IEEE SA's Meta Issues in Cybersecurity Industry Connection.

1.2. RECOMMENDATIONS

1.2.1. PURPOSE

IEEE's goal of advancing technology for humanity provides both hope and promise. Attacks on cybersecurity appear to be growing at a faster rate than the uptake of digital technology. If this trend continues, economic and national security will be severely impacted within a few years due to the world's digital resources experiencing irrevocable cybersecurity damage. This will force companies, governments, and users to retreat to separate gated digital neighborhoods or participate at personal risk. Improved cybersecurity is aligned with IEEE's goal.

The idea of protecting all cyberspace is important in the cybersecurity field, given the predominance of common technologies and interconnected cyberspace. A vulnerability discovered in any location may quickly become exploited globally. When two countries fight over territory, one country's gain is the other country's loss, a zero-sum game. In cyberspace, however, a new technology that strengthens cybersecurity benefits all. A new exploit is a detriment to all. In the context of IEEE's pledge to advance technology for humanity, the chronic state of cybersecurity vulnerability may be viewed as a threat to the benefits humanity can otherwise expect.

Recommendation 1: IEEE should link dependency on cybersecurity to the achievement of our goal of advancing technology for humanity.

1.2.2. INDEPENDENCE

IEEE has members in 160 countries. Essentially, IEEE members can be found wherever advanced technologies are being developed or implemented. Most people in the world benefit from IEEE standards every day. They

[16] "Common Vulnerability Scoring System SIG," FIRST — Forum of Incident Response and Security Teams, accessed December 27, 2022, https://www.first.org/cvss.
[17] "OWASP Top Ten | OWASP Foundation," accessed December 27, 2022, https://owasp.org/www-project-top-ten/.

Documents Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

promote the beneficial use of technology generally. In this, IEEE is distinct to governments, whose responsibility is to protect a national interest, and companies, whose focus is commercial interest. As a result, cybersecurity vendors are conflicted, as increase in cyber investment drives increase in prices and could lead to decline in sales due to affordability; cybersecurity training certification bodies benefit from the largest number of certification holders, not necessarily the best training; technology device manufacturers are usually not penalized for poor security; consumer and competition regulators are under-informed; policing units are enormously under-trained; standards organizations to date are limited to spot or partial solutions; associations of security professional lack a global voice; and academic researchers focus on pieces of the puzzle. In addition, governments spend large investments in building offensive security capabilities due to national security interests. This report identifies significant opportunities for collaboration in industry, academia, and government.

Recommendation 2: IEEE should apply its reputation for independence to establishing effective cybersecurity principles and standards.

1.2.3. BREADTH

An enormous proportion of the world's resources are devoted to the development of technologies, and as a result, advanced technologies are becoming less predictable, isolated, and mechanical, and more intelligent, distributed, and social. IEEE members are found in all these fields, from power to quantum to societal. Cybersecurity is attacked at its weakest links. An approach cannot assume that digital technologies are independent of their physical environment, or that because an enterprise operates in silos, attackers are similarly constricted. IEEE has members working across the technology stack and, therefore, has the capacity to conceptually bridge the apparently unconnected. In its efforts on this topic, IEEE attempts to operate in a country or industry-agnostic manner with the sole aim of advancement of technology for humanity.

Recommendation 3: IEEE should encourage a broad approach to cybersecurity, not just obvious vulnerabilities, reflecting the breadth of its members' expertise.

1.2.4. EXPERIENCE

IEEE plays an important part in the development of cybersecurity technology practice, including IEEE Std 2410™ for biometric authentication in financial services. It publishes three of the top four cybersecurity journals, has a wide range of conferences, educational activities, and key volunteers, and IEEE members have a broad interest in cybersecurity. Nevertheless, these significant achievements are fragmented, partial, and localized. A listing of

Documents
Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

92 cybersecurity industry and professional associations does not list IEEE.[18] In a quick search of 31 professionals listed in a cybersecurity hall of fame,[19] only two identify as IEEE members, and only half have had any obvious connection with IEEE, such as publishing or speaking at IEEE activities. Another list of influential figures to follow in 2021 tells the same story.[20] IEEE has not yet brought the message of advancing technology for humanity to the cybersecurity field.

Recommendation 4: IEEE should use its areas of deep experience to encourage cybersecurity specialists to make IEEE their professional home.

2. FROM WHERE DO VULNERABILITIES COME?

The continuing erosion of cybersecurity reflects a series of challenges faced in the production of online products and services. This can be contrasted, for example, to the increasing effectiveness of safety devices in transport technologies. Poorly aligned reward structures include the following:

Lack of Product Liability: The absence of liability for the release of insecure products results in a secure design becoming a burden for a company not shared by its insecure competitors. This should not be the case. Across the world, safety standards for devices have been adopted. Seatbelts and airbags are regularly fitted to vehicles, and lead additives have been removed from fuel. The use of lead paint on children's toys, of small parts in toys that could lead to choking, food adulteration, or flammable material in night-clothing, is now widely rejected. Yet it remains legal to release known significant cybersecurity flaws. The buyer may or may not be under an obligation to accept a safe product, but they may also be rewarded for selecting a low-cost product.

Lack of Regulation Requiring Secure Devices: The selection of products based on price rather than security may require a regulatory response. For example, a Californian IoT statute establishing a very simple benchmark, no default passwords, is a first step in addressing the notorious insecurity of IoT consumer devices.[21] IoT devices are both low in power and low in processing capability, a poor start for security. Their protection, therefore, cannot be based on an expectation that they can individually repel a sophisticated attack. IoT vulnerabilities also

[18] "List of Cybersecurity Associations and Organizations," *Cybercrime Magazine* (blog), February 28, 2018, https://cybersecurityventures.com/cybersecurity-associations/.
[19] https://www.infosecurityeurope.com/en-gb/whats-on/hall-of-fame.html
[20] https://www.balbix.com/insights/top-cybersecurity-influencers/
[21] Dean Sysman, "Council Post: California's IoT Security Law: Why It Matters And The Meaning Of 'Reasonable Cybersecurity,'" Forbes, accessed December 31, 2021, https://www.forbes.com/sites/forbestechcouncil/2019/11/20/californias-iot-security-law-why-it-matters-and-the-meaning-of-reasonable-cybersecurity/.

Documents Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

raise the question, who is at fault when compromised firmware in an IoT consumer device is not updated? Clearly, not the consumer.

Competitive Rather Than Cooperative Approach to Cybersecurity: There are limited benefits for companies collaborating on the adoption of secure architecture, standards, and processes, and no perceived value in voluntarily sharing information about a cyber-attack. Depending on the political or commercial need, a human error or natural disaster may be blamed on a cyber-attack, or vice versa.[22] Cybersecurity is seen as a zero-sum game, the more security I have, the less you have. On the contrary, cybersecurity is the tide that lifts all boats. The less vulnerable you make your products, the more secure are my products.

Cybersecurity as an Add-On: In the 1960s, packet-switching architect Paul Baran stated that security had to be built in from the beginning; it could not be effectively added at the end.[23] This truism of cybersecurity design still evades us.

Motive and Opportunity: Cybercrime shares many traditional characteristics of traditional financial crime, and motives such as inequality provide a strong driver for participants. At the same time, training millions of people in cybersecurity in a short time without a strong ethical or other professional tradition provides the tools for the very crimes that are sought to be prevented.

Lack of a Professional Outlook: While cybersecurity vulnerabilities are found in many places—technical, psychological, sociological, criminological, legal, and others—the cybersecurity profession has not established itself to encompass all of these. Rather, it is generally a subset of information technology (IT). Until the profession establishes an appropriate identity, for example, following models of the medical, legal, or accounting professions, it will be only partially fit for its task.

Blaming Human Error: Although the great majority of cybersecurity incidents involve social engineering, convincing a person to "open a door" for the attacker, it does not follow that the person is at fault. Cybersecurity design that depends on a vigilant user to make up for the technology environment's inherent cybersecurity weaknesses is poor cybersecurity.

Poor Alignment Between Technical Skills and Need: WEF 2021 estimated an international shortage of more than 3 million cybersecurity professionals.[24] One year later, a longitudinal study by Cybersecurity Ventures

[22] Mike Johnstone, "Did the Census Really Suffer a Denial-of-Service 'Attack'?," The Conversation, accessed December 31, 2021, http://theconversation.com/did-the-census-really-suffer-a-denial-of-service-attack-63755.
[23] Paul Baran, "On Distributed Communications," August 1964.
[24] https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/

Documents Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role

arrived at a similar figure of 3.5 million.[25] This reflects the gap between rising demand and current training. However, there are also some systemic problems. For example, without cybersecurity literate teachers and professors, there is no simple way to achieve the necessary skills training. Self-serve training, both open source and commercial, is available but depends on the motivation and resources of the individual. In some areas, such as policing, while most modern crime has a cyber aspect, just a few percent of police globally have cybersecurity training.

3. WHAT IEEE CAN BRING TO CYBERSECURITY

While IEEE currently lacks an ongoing cybersecurity identity, its diverse organizational units (OUs) have created an enormous collection of research and industry artifacts that clearly establish the claim that IEEE is an important contributor to cybersecurity, even if not widely recognized as such.

3.1. IEEE AS A PLATFORM FOR CYBERSECURITY ACTIVITY

IEEE and the Cyber-Physical: Modern cybersecurity approaches, including the IoT, quantum, and critical infrastructure, involve both digital and analog technologies. This can be described as the intersection of engineering and computer science or of IT and OT. Covering both in its core fields of interest, IEEE is therefore in a strong position to address end-to-end technical challenges in cybersecurity.

IEEE is Nationally and Commercially Neutral: A significant change in the cybersecurity field in recent years has been the role of nation-states. Advanced persistent threats (APTs), for example, refer to actors who have effectively unlimited budgets to fund cybersecurity attacks, eliminating the assumption that an adversary will only spend as much on an attack as they reasonably believe they can gain. While IEEE has legal obligations within the United States, its declared allegiance is to the global profession. IEEE places no ideological, national, commercial, or religious precondition on its goal of advancing technology for humanity. This enables it to

[25] Sydney Lake, "Companies Are Desperate for Cybersecurity Workers," Fortune, July 1, 2022, https://fortune.com/education/articles/companies-are-desperate-for-cybersecurity-workers-more-than-700k-positions-need-to-be-filled/.

Documents
Document Sharing Hub
Copyright © 2023 IEEE. All rights reserved.
Full document details: IEEE and the Protection of Cyberspace: Increasing IEEE's Cybersecurity Role