Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

Agenda

This conference will enable the sharing of cybersecurity expertise, strategies, and lessons learned from the United States, Poland, Georgia, Romania, Croatia, and Ukraine on preventing, detecting, and responding to the cybertheft of research, data, intellectual property, and technologies considered critical and dual-use.

Through panels, presentations, and workshop sessions, the conference will increase knowledge and awareness of specific cyberthreats, foster dialogue between key stakeholders across sectors and multiple countries, and support practical steps that address threats to the research and technology sectors.

Who Should Attend?

- Public Sector: Governmental research funding and support, ministries of education, science, and technology, cybersecurity and regulatory authorities, national CERTs
- Research Sector: University leaders and administrators, department heads, research project directors, university faculty, laboratory directors, compliance office managers, IT and cybersecurity managers
- Private Sector: Technology and private research company executives and managers, IT and cybersecurity managers

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 1

08:00 – 09:00	ARRIVAL & REGISTRATION
09:00 – 09:45	*OPENING PLENARY* *Featuring keynote speeches by high-level decision-makers and experts, following the leitmotif of the conference – prevention of data, intellectual property, and technology theft.* US Representative, EU Representative, Polish Government Representative, Academia Representative
10:00 – 10:45	*PANEL DISCUSSION* *THE CYBER THREAT LANDSCAPE: 2022 TO 2023* *Researchers, academic institutions, and the private sector face increasing threats of cyberattacks every year. The dominant threat now comes from foreign governments sponsoring cyber actors to steal sensitive data, research, and intellectual property (IP) from institutions to gain access to key critical and dual-use technology. Armed with state-provided resources, these cyber threat groups pose a significant risk to open and secure science, research, and technology development. What were the biggest cyber threats in 2022? What trends and attack vectors have we observed against different sectors of industry and government? What were the motivations of the attackers and what impact did the cyberattacks have on the research and technology sectors? What types of intellectual property and data have been most targeted?*
11:00 – 11:45	*PANEL DISCUSSION* *CYBERESPIONAGE: INTERCONNECTED THREATS AND VULNERABILITIES* *Researchers, academic institutions, and the private sector face increasing threats of cyberattacks every year. The dominant threat now comes from foreign governments sponsoring cyber actors to steal sensitive data, research, and intellectual property (IP) from institutions to gain access to key critical and dual-use technology. Armed with state-provided resources, these cyber threat groups pose a significant risk to open and secure science, research, and technology development. What were the biggest cyber threats in 2022? What trends and attack vectors have we observed against different sectors of industry and government? What were the motivations of the attackers and what impact did the cyberattacks have on the research and technology sectors? What types of intellectual property and data have been most targeted?*

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 1

12:00 – 13:00	*PANEL DISCUSSION* *CYBERSECURITY OF DUAL-USE RESEARCH & TECHNOLOGY SUPPLY CHAINS* *With the rise of regional geopolitical unrest and increased military spending in countries worldwide, the cybersecurity of dual-use technologies is crucial to maintaining national security. Public-private partnerships are critical to the effective development of the defense sector, but this also means a much greater risk for service providers and products that state and non-state malicious actors can target. How can both government and their non-government partners in the research and private sectors ensure the security of supply chains of strategically essential technologies, including in areas such as robotics, artificial intelligence, autonomous systems, sensors etc.? How can countries cooperate in setting security rules for emerging and disruptive technologies?*
13:00 – 14:00	LUNCH
14:00 – 14:45	*PANEL DISCUSSION* *A "TRIPLE HELIX" APPROACH TO CYBERSECURITY: HOW CAN PARTNERSHIPS BETWEEN STATE, BUSINESS, AND ACADEMIA ENHANCE CYBERSECURITY?* *In an increasingly digitalized world, cooperation between multiple stakeholders is needed to ensure cybersecurity. The "triple helix" form of collaboration, involving the cooperation of actors from government, the private sector, and academia, has proven extremely successful in many areas beyond cybersecurity. This approach, which allows knowledge, expertise, lessons learned, and costs to be shared in order to develop the best possible solutions, may be particularly useful in the cybersecurity environment, due to constantly evolving challenges and risks requiring the involvement, resources, and efforts of multiple stakeholders. What are examples of successful cooperation and partnership among these sectors? How might this approach be promoted to enhance approaches against cybertheft? Who are the key stakeholders in these processes? What should be prioritized and how can collaboration best be facilitated? What obstacles and solutions are there related to legislation and institutional cooperation?*

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 1

15:00 – 15:30	*PRESENTATION* *CYBERSECURITY CULTURE: HOW TO FOSTER AT YOUR ORGANIZATION* *Cybersecurity culture is essential in creating a secure research environment that can still foster collaboration. It means that every employee shares the same set of values, procedures, and behaviors that promote the confidentiality of information and help protect the assets from various cyberthreats. It also means that everyone in an organization is aware of the importance of cybersecurity and their role in prevention of security breaches, their responsibility with complying with relevant regulations and internal procedures, and the impact of possible breaches. How can institutions best educate employees on the importance of cybersecurity and on their roles? How can basic cyber hygiene practices prevent the most common cybertheft vectors? How can organizations establish proper policies and procedures on handling sensitive data and intellectual property? What are successful examples in the research and private sectors, and are there major differences in approaches? How can organizations encourage a culture of vigilance? How can institutions ensure that security measures are aligned with industry best practices?*
15:30 – 16:00	AFTERNOON BREAK
16:00 – 16:45	*PANEL DISCUSSION* *CYBER RESILIENCE RISK MANAGEMENT* *Cybersecurity is a collective, on-going effort that should be an overarching mission within every department in an organization. All personnel are vulnerable to cyberattack and each has a role to play in keeping research and information at the organization safe. Maintaining up-to-date and agile risk management is critical to an organization's security in the ever-evolving threat landscape. How should a whole-of-organization approach to cyber security be structured? What are the risks faced by each department or function? How to deal with a large number of devices and users assessing sensitive data from various locations? How to safely collaborate with external partners? How is risk assessed and dealt with in different countries and sectors?*

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 1

17:00 – 17:30	*PRESENTATION* *NEW AGE OF CYBERSECURITY: HOW WILL QUANTUM REVOLUTION AFFECT SECURITY?* *The quantum revolution could have huge implications for cyber security. Encrypted data, stolen in hacking attacks, could be decrypted using quantum computers in the future. A number of countries, led by the US, are already starting to implement post-quantum cybersecurity standards. How should states and research institutions prepare for the changes brought about by quantum computers? What is there to be done about it right now? What legislative changes do we need? How should the state work together to prevent encryption breaches?*
17:30 – 20:00	NETWORKING RECEPTION

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 2

09:30 – 10:00	ARRIVAL & REGISTRATION
10:00 – 10:45	*PANEL DISCUSSION* *CYBERSECURITY OF RESEARCH INSTITUTIONS: NATIONAL POLICIES AND APPROACHES* *Research institutions remain one of the main targets of cyberattacks, due to sensitivity and amount of data they possess and manage on a daily basis. The problem was particularly evident in the first months of the COVID-19 pandemic with many attacks targeting vaccine and drug development facilities. National frameworks are one of the main sources of regulation and technical standards to follow for research institutions to secure their systems, networks and databases, and prevent incidents that could lead to data theft or manipulation of information. Countries have different experiences and standards often driven by larger multistakeholder organization frameworks. This panel discussion will review the key elements of national cybersecurity frameworks as they apply to research institutions and allow for sharing knowledge and lessons learned to-date. It will examine challenges faced and methods of successful collaboration between government and industry in addressing emerging threats.*
11:00 – 11:30	*PRESENTATION* *DEALING WITH CYBERSECURITY BREACHES* *The accelerated digital transformation has expanded the threat landscape in an unprecedented way, bringing new challenges and risks to organizations' cybersecurity systems. In times where a single misstep and loophole can invite hackers into critical systems, networks and databases, preventing cyber incidents is a difficult task. This presentation will examine various types of cybersecurity breaches that organizations may face and the key steps that need to be taken in the aftermath. It will discuss investigation, identification of vulnerabilities, mitigation of effects, recovery, restoration of services, ways to communicate with partners and regulators, responsibilities of mid- and senior management and their decision-making process and the importance of incident response plans.*
11:30 – 12:00	MORNING BREAK

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 2

12:00 – 12:30	*PRESENTATION* *HOW TO SAFELY INTRODUCE & MANAGE CLOUD-BASED SERVICES IN SENSITIVE DATA ENVIROMENTS?* *Many institutions shy away from putting their data, especially sensitive data, in the cloud. Despite the rapid development of these technologies, the vision of storing data on third-party servers is a stumbling block for many public, private, and academic institutions, especially those working with dual-use technologies. Should we be afraid of public clouds? Is it possible to do so securely in a sensitive data environment? How vulnerable are they to cybertheft? How can institutions properly procure and audit these services?*
12:45 – 13:30	*PANEL DISCUSSION* *STRENGTHENING WEAK LINKS: HOW TO SET SECURE RULES FOR SUPPLIERS AND CONTRACTORS?* *Attacks on supply chains are among the most common and largest threats to information security in cyberspace, with the likes of the SolarWinds hack and Microsoft Exchange Server attacks. Businesses, academia, and government decision-makers need to ensure that the providers of their services and products are taking appropriate care of cybersecurity. How can we make sure that we mitigate any vulnerabilities in supply chain links? How to carry out a practical yet effective risk assessment process and what to look for in particular? How to make sure that data shared with a provider have similar secure authentication and access controls?*
13:30 – 14:30	LUNCH

Conference on Preventing the Cybertheft of Research and Technology

13-14 April, 2023
Warsaw, Poland

DAY 2

14:30 – 17:30	*WORKSHOP* *Workshop leader: Eric Novotny, Ph.D.* *The workshop session will combine elements from the previous sessions on research and cybersecurity into an engaging, group-focused opportunity for establishing goals, priorities, plans and procedures. This will include questions on cross-sectoral cooperation, regulatory and policy, implementation challenges, training needs, and measuring outputs. The session will focus on specific areas of responsibility and will then allow plans and priorities to be compared and discussed. Specialized groups will reveal their proposed actions, their expectations from the other sectors, and gaps that may need to be filled. The workshop will allow participants to join one of the five groups, depending on their affiliation or interests. Planned activities will include group work, findings presentation, and general discussion.*
17:30 – 20:00	NETWORKING RECEPTION

Point of Contact:

Ihor Andrusyk
Project Lead, CRDF Global
iandrusyk@crdfglobal.org

Roman Komyna
Project Associate, CRDF Global
rkomyna@crdfglobal.org

cyberseccconf23@crdfglobal.org