Research Security 360

A Complete View

John Nord, CITO at Cayuse

Agenda

1. Why Research Security?
2. Current State of Research Security
3. A Holistic View
4. Action Plan for Compliance
5. Wrap-Up
6. Q&A

Why Research Security?

Why is securing our research vital?

(national defense, stolen IP, loss of funding, etc)

National Defense Authorization Act (NDAA) highlights the need to enhance technologies (research) while protecting this intellectual capital (IC) and intellectual property (IP) from foreign entities – the DoD receives about $95 billion annually to fund research and development efforts (link)

IC and IP theft – the first to file conundrum – estimated to cost US businesses and institutions in excess of $600 billion annually. Dealing with both insider and external threats

Why Research Security?

Total value of R&D (in USD)

Total Spend in U.S. (2022) = ~$886 Billion

Total Global Spend (2022) = ~$2.5 Trillion

Table 2

Higher education R&D expenditures, by source of funds: FY 2022

(Millions of current dollars)

Source of funds	2022	% of total
All R&D expenditures	97,681	-
All federal R&D expenditures	53,971	55.3
DOD	7,979	8.2
DOE	2,488	2.6
HHS	30,289	31.0
NASA	2,044	2.1
NSF	6,036	6.2
USDA	1,501	1.5
Other	3,635	3.7
All nonfederal R&D expenditures	43,709	44.8
State and local government	4,907	5.0
Institution funds	24,493	25.1
Business	5,702	5.8
Nonprofit organizations	5,974	6.1
All other sources	2,633	2.7

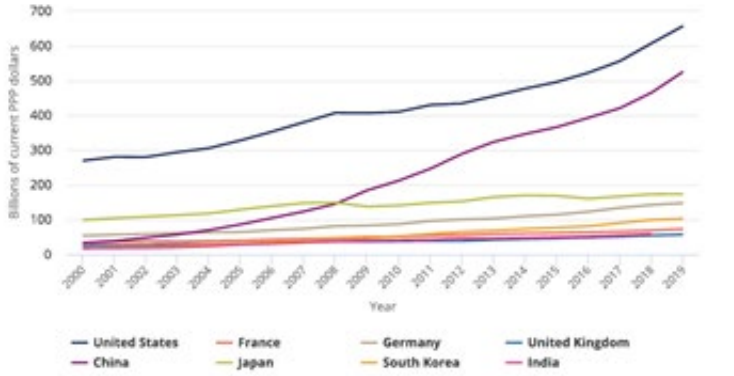
Higher Education Expenditures (https://ncses.nsf.gov/pubs/nsf24307)

Why Research Security?

National Center for Science and Engineering Statistics | NSB-2022-1

Figure 12

Gross domestic expenditures on R&D, by selected country: 2000–19

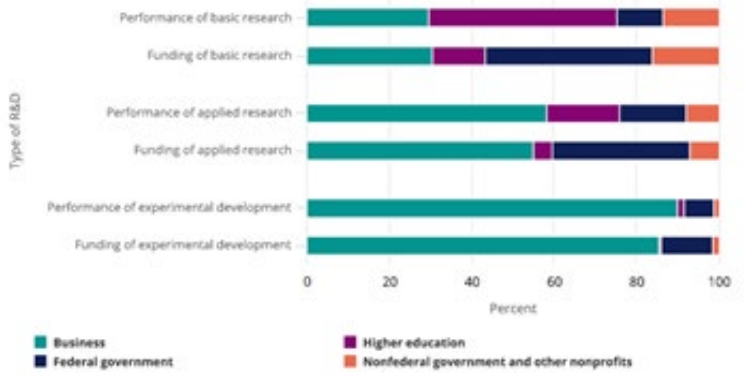


Note(s):
PPP is purchasing power parity. Data are for the top eight R&D-performing countries. Data are not available for all countries for all years. Gross domestic expenditures on R&D were revised from those reported in previous years of *Science and Engineering Indicators*. These data revisions were mostly due to 2020 revisions of the PPP estimates. See sidebar Revisions to Global Research and Development for more details.

Source(s):
NCSES, National Patterns of R&D Resources; OECD, MSTI March 2021 release; UNESCO, UIS, R&D dataset.

Indicators 2022: R&D

Figure 18. U.S. R&D performance and funding, by type of R&D and sector: 2019



Note(s): The data for 2019 are estimates and will later be revised.

Source(s): NCSES, National Patterns of R&D Resources, 2019. *Indicators 2022: R&D*

National Science Board Report (https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-research-and-development)

Current State of Research Security

Recent Fines, Compliance, and Security Issues

Feds hit Penn State University with false claims lawsuit over cyber compliance

U.S. NEWS OCT. 2, 2023 / 11:49 PM / UPDATED OCT. 3, 2023 AT 9:50 PM

U.S. fines Stanford $2M for failing to disclose foreign research funds

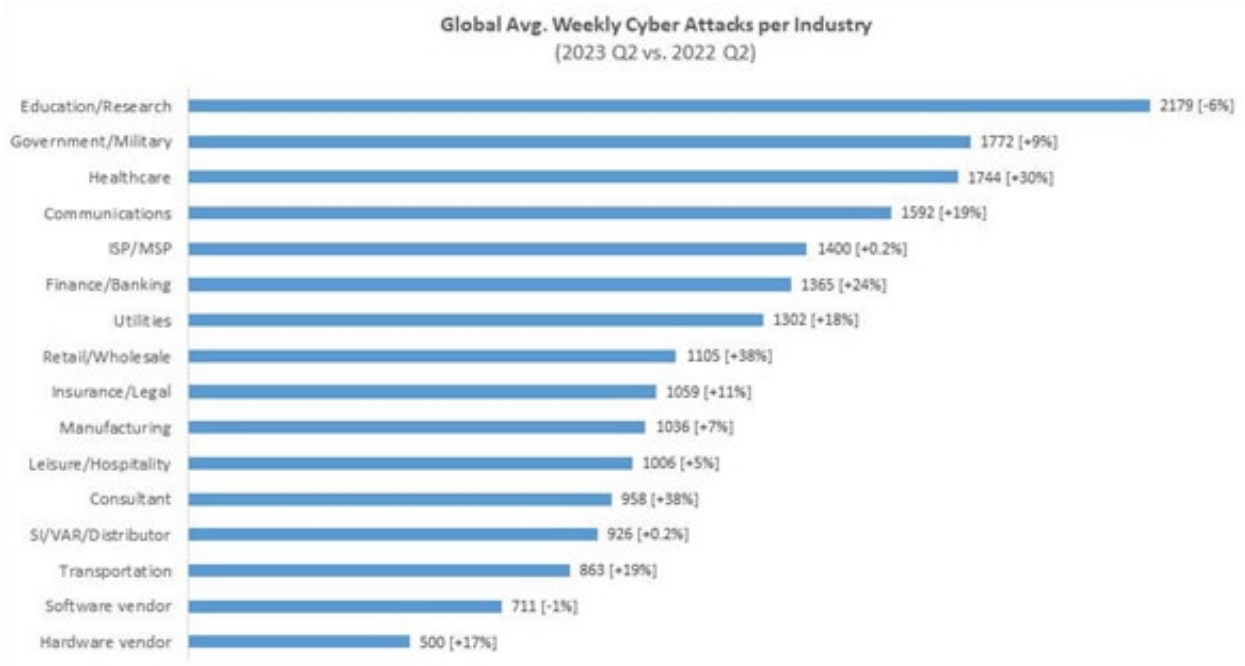
NASA Researcher Arrested for False Statements and Wire Fraud in Relation to China's Talents Program

Manchester University Breach Victims Hit with Triple Extortion

Current State of Research Security

National Science Foundation (https://new.nsf.gov/research-security#violations)

Current State of Research Security



Checkpoint (https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/)

The Secure Research Wheel

A Holistic View

Security is more than just “Research” Security – important to remember that

Regulations, regulations, regulations (NSPM-33, CHIPS and Science Act of 2022, NIST, NISPOM, FAR, DFARS, FCI, CUI, etc.)

- What do we need to do to keep our research compliant?
  - Training, Disclosure Management, Foreign Visitors, Export Controls, etc.
  - Don’t forget about Cybersecurity!
- Lots of various compliance frameworks, regulations, mandates, and specific requirements
- Security is still security – don’t forget the basics – commonalities across the alphabet soup
- Research Security does not equal Total Compliance
- Protecting the actual research activities after grant award

A Holistic View

Bid/No Bid and Contract/Award reviews – catching gotcha statements and the potential use of AI

AI is the newest buzzword, but can it help us speed up the review process?

Short answer, yes.

Key points to understand, in regards to overall security and compliance:

- **Security Language**
  Pay attention to specific frameworks, regulations, mandates, etc.
- **Technology and Data Requirements**
  Restrictions on data transfers, classification of data, special data handling requirements, data retention requirements, types of technologies needed for data sharing,
  data residency requirements, etc.

Action Plan for Compliance

Trust, but Verify – COI and Foreign Influence

- Go beyond self-attestation – take the next step with modern tools
- Communication at all levels w/ centralized information at the research institution level

Training, training, and then Follow-up (possibly with training)

- Should be treated like CITI or other training platform you use
- Create or buy - that is the question

Action Plan for Compliance

Research security beyond the Research (data, compute, lifecycle management) – including in bids

- An overall compliant security program is research security
- We protect against foreign influence and other aspects of research security now what
- The research compute and data lifecycle – it doesn't stop when the research grant stops

Internal or External (it depends) – initial setup is possible, upkeep is costly/challenging

- Build vs. Buy - pros/cons; what happens if the builder leaves?
- Ongoing upkeep can get costly - personnel, infrastructure costs, security costs
- Risk Assessments and Risk Tolerance
  - Accept, Transfer, Mitigate, or Avoid (choose wisely)

Action Plan for Compliance

Dotting i's and crossing t's – the assessment/checklist method

- Need to develop "checklist" action plan
- General items should include:
  - Research Program Policies and Procedures
  - Research Training
  - Check and verify foreign influence and conflicts of interest
  - Review compliance requirements in research award
  - Work with IT and Security group to verify compliance
  - Decide on build vs. buy for research effort technology/security
  - Validate solution to contract requirements
  - Audit regularly to make sure commitments are still met

Sample Risk Management Plan

IPTalons and Cayuse offer a proactive approach to assessing and managing risks in research programs, ensuring **compliance** with regulations, identifying potential **conflicts of interest**, evaluating **supply chain vulnerabilities**, and addressing **foreign influence threats**.

Through **comprehensive assessments** and **targeted analyses**, we provide **actionable insights** to enhance the security and resilience of your organization's research endeavors.

Insider Risk and Research Program Assessments

Foreign Affiliation COI Disclosure Veracity Check

CMMC Gap Assessments

Due Diligence and Supply Chain Analysis

Foreign Influence Threat Finder

Wrap-up

Security is Security (75%+ is standard, it's the specialized part that can get you)

We want to make headlines – just not in that way

Compliance takes investment and support

Adapt the action plan to fit your organization's needs – buddy up with your organization's IT and security team(s)

Q&A

References

Check Point Team. (2023, July 13). Average Weekly Global Cyberattacks peak with the highest number in 2 years, marking an 8% growth year over year, according to Check Point Research. *Check Point.* https://blog.checkpoint.com/security/average-weekly-global-cyberattacks-peak-with-the-highest-number-in-2-years-marking-an-8-growth-year-over-year-according-to-check-point-research/

Coote, D. (2023, October 3). U.S. fines Stanford $2M for failing to disclose foreign research funds. *UPI*. https://www.upi.com/Top_News/US/2023/10/02/Stanford-fine-foreign-sources/2211696302222/

Gibbons, MT; National Center for Science and Engineering Statistics (NCSES). 2023. R&D Expenditures at U.S. Universities Increased by $8 Billion in FY 2022. NSF 24-307. Alexandria, VA: National Science Foundation. Available at https://ncses.nsf.gov/pubs/nsf24307.

Johnson, D. (2023, September 14). Feds hit Penn State University with false claims lawsuit over cyber compliance. *SC Magazine.* https://www.scmagazine.com/news/feds-hit-penn-state-university-with-false-claims-lawsuit-over-cyber-compliance

Lanhee Lee, J. & Psaledakis, D. (2021, February 28). U.S. doubles down on protecting university research from China. *Reuters*. https://www.reuters.com/world/china/us-doubles-down-protecting-university-research-china-2021-03-01/

Muncaster, P. (2023, June 23). Manchester University Breach Victims Hit with Triple Extortion. *Infosecurity Magazine.* https://www.infosecurity-magazine.com/news/manchester-university-victims/

References

OECD (2022), "Integrity and security in the global research ecosystem", OECD Science, Technology and Industry Policy Papers, No. 130, OECD Publishing, Paris, https://doi.org/10.1787/1c416f43-en

U.S. Department of Justice. (2020, August 24). NASA Researcher Arrested for False Statements and Wire Fraud in Relation to China's Talents Program. https://www.justice.gov/opa/pr/nasa-researcher-arrested-false-statements-and-wire-fraud-relation-china-s-talents-program

U.S. Government Accountability Office. (2023, June 29). *Research and Development: DOD Benefited from Financial Flexibilities but Could Do More to Maximize Their Use.* https://www.gao.gov/products/gao-23-105822

U.S. National Science Foundation. (n.d.). *How NSF addresses research security violations.* https://new.nsf.gov/research-security#violations

United States Senate Committee on Armed Services. (n.d.). *Summary of the Fiscal Year 2024 National Defense Authorization Act.* https://www.armed-services.senate.gov/imo/media/doc/fy24_ndaa_conference_executive_summary1.pdf