**FBI Mission**  
*To protect the American people and uphold the constitution of the US*.

To start each fiscal year, the FBI identifies threats affecting each territory and determines how best to utilize resources. In doing so, we recognize that to truly operate in that space before an incident/attack happens, we need to influence corporate culture and behavior by getting in front of the decision makers: the executives.

We can AND DO share indicators of compromise everyday with your IT staffs, HR departments, etc. BUT to truly disrupt the threats we ALL face, YOU (executives) need to hear about them and understand how 1) to change the security hygiene of your organization for the better and 2) how to leverage the FBI as a resource in creating your security game plan. #taxpayermoney@work

**Investigative priorities**

* Protect the US from terror attack
* Protect the US from counterintelligence/espionage
* Protect the US from cyber-based attack
* …

**FBI Cyber mission**

* To impose risk and consequence on cyber adversaries through unique authorities, world-class capabilities, and enduring partnerships, building on a century of innovation.

**FBI Definition of Cybercrime**

* Financially motivated
* Non-financially motivated
* Nation-state | Government sponsored
  + China, Russia, Iran, and North Korea

**China Threat**

* A link to Director Wray’s speech regarding the China Threat from July 7, 2020[: Click here.](https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states)
* A link to H.R. McMaster’s excerpt from his book Battlegrounds: The Fight to Defend the Free World: [Click here](https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/).
* It is very important that we realize that China has a PLAN (https://www.uscc.gov/trade-bulletins/april-2021-trade-bulletin) to strengthen their country. ALL citizens are required to see the plan through: [Click Here](https://www.uscc.gov/trade-bulletins/april-2021-trade-bulletin).
* Fall of 2018, 10 Chinese government officials from MSS were indicted (<https://www.justice.gov/opa/press-release/file/1106491/download>)
* As a result of these indictments, the DOJ unveiled the China Initiative (<https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage>) which basically states that the US is tired of China brazenly weakening our global economic position.
* The July 21, 2020 announcement of the Indictment of two Chinese Hackers alleging they targeted Intellectual Property, including COVID-19 research: [Click Here.](https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion)
* Suggested Reading: The Hundred-Year Marathon: China’s Secret Strategy to Replace America as the Global Superpower, by Michael Pillsbury (2015).

**Cyber Reports**

Some of the statistics within the presentation are from the following reports. In some instances, the reports are free but you may have to enter an email address to download:

* [Accenture: Cyber Threat Intelligence Report 2021](https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50)
* [IBM Cost of a Data Security Breach Report 2021](https://www.ibm.com/security/data-breach)
* [IBM X-Force Threat Intelligence Index 2021](https://www.ibm.com/security/data-breach/threat-intelligence)
* [2020 IC3 Annual Internet Crime Report](https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)
* [2021 Verizon Data Breach Investigations](https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf)

**Ransomware**

* 2020 version of Organized Crime
  + Safer and **MUCH** more lucrative
* FBI recommendation - is to get ‘Left of Click’ and have valid/working backups
* Recent change in tactics involve "Big Game Hunters"
  + Cities, municipalities, and infrastructure being targeted (i.e. TEXAS)
  + Ransomware Prevention and Response for CEOs <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view>
  + <https://www.cisa.gov/stopransomware>
* Open-Source Decryptors – (For Information only, not official endorsed by the FBI)
  + NoMoreRansom <https://www.nomoreransom.org>
  + The Windows Club <http://wwwthewindowsclub.com>
  + Cisco <http://www.talosintelligence.com/teslacrypt_tool/>
  + McAfee http://www.mcafee.com/us/downloads/free-tools/shadedecrypt.aspx

**BEC**

* Biggest scam currently affecting this country
* San Diego prosecutors (Federal) won’t take a case with losses <$400K
* Attached to the email please find the CEO Wire Fraud Checklist
* If your company is targeted and money is wired, contact FBI immediately...
  + Immediately = within 3 days
    - Either call local FBI or...
  + Logon to [www.ic3.gov](http://www.ic3.gov/) and file a report – similar to a police report
  + The above steps will activate a financial ‘kill chain’ and the odds of getting your money back greatly increase

**Insider Threat**

* Be aware of visitor benefits/risks. Consider developing a response plan and/or protocol when hosting foreign investors/visitors. Feel free to use this resource - <https://www.fbi.gov/file-repository/risks-mitigations-of-visitors-brochure.pdf/view>
* Understand the Insider Threat. This can mean MANY different things and come from many vectors: disgruntled employee, fired/released employee, strategically placed investor/visitor, etc.
  + For additional context, please see <https://www.fbi.gov/file-repository/insider_threat_brochure.pdf/view>

**SolarWinds Orion**

[Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence (ODNI)](https://www.fbi.gov/news/pressrel/press-releases/joint-statement-by-the-federal-bureau-of-investigation-fbi-the-cybersecurity-and-infrastructure-security-agency-cisa-and-the-office-of-the-director-of-national-intelligence-odni)

[CISA Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise](https://cyber.dhs.gov/ed/21-01/)

[CISA Supply Chain Compromise](https://www.cisa.gov/supply-chain-compromise)

**International Travel for Executives**

* We talked about 'burner laptops' and understanding the possibilities that you, as executives, "may" be targeted when traveling to 'unfriendly' countries.
* Be aware of individuals providing you with *materials* for the purpose of being stopped by authorities for possessing those *materials*.
* Leverage the State Department's travel advisories (<https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/>) prior to ANY international travel.
* Please download and share this brochure - <https://www.fbi.gov/file-repository/business-travel-brochure.pdf/view>

**Additional Information:**

* **The FBI’s Protected Voices initiative provides tools and resources to political campaigns, companies, and individuals to protect against online foreign influence operations and cybersecurity threats. While these instructional videos were created for political campaigns, they can be applied to any sector. One could use these videos to kick start training for employees regarding cybersecurity.**
* <https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices>

**DHS: Cybersecurity & Infrastructure Security Agency**

* **For more information:** [**www.CISA.gov**](http://www.CISA.gov)

**Final Note(s)**

* When do I call the FBI?
  + You should call your local FBI BEFORE an incident
  + Much better to have a contact than to rummage thru a call tree while things are blowing up internally.
* The FBI is much more than the Executive Briefing Series. We have MANY outreach programs that you AND your family can take advantage of (<https://www.fbi.gov/about/community-outreach>)
  + Junior Agent program
  + Teen Academy
  + [InfraGard](https://www.infragard.org) (www.infragard.org)
    - Free and offers you the opportunity to partner with peers in your territory AND the FBI
    - You also will receive intelligence classified at the FOUO (FOR OFFICIAL USE ONLY) level
    - AND excellent training in all things security (both cyber AND physical)
  + Citizens Academy
* If you happen to see any of these individuals (<https://www.fbi.gov/investigate/cyber/most-wanted> AND <https://www.fbi.gov/wanted>) please give us a call soonest!

**Contact**

If you have any questions or concerns, feel free to contact me at [njarico@fbi.gov](mailto:njarico@fbi.gov). (Even if the issue is not a Cyber matter, I can get you the information or in front of the person that can help you)

SSA Nicholas Arico

FBI San Diego

njarico@fbi.gov