HEALTHCARE INNOVATION CAPITAL: INSIDER THREATS & CYBER ESPIONAGE

Brief:

Foreign Adversaries are aggressively using novel mechanisms to acquire intellectual property, research, and sensitive technology. Not only have nation state threat actors cultivated and leveraged advanced cyber-espionage capabilities, but they have also built robust human Intelligence (HUMINT) programs to accomplish their goals. Those programs are used to gather intelligence to start or enhance state-run programs to manufacture, re-design, enhance, or otherwise improve existing products and infrastructure.

Organizations should expect foreign adversaries to target developmental processes as well as individuals in order to obtain privileged access to information. Foreign adversaries could target merger and acquisition negotiators or negotiation strategy to gain a competitive economic advantage. Supply-chain attacks are an on-going threat to entities which rely on third-party organizations for operational support.

Foreign Adversaries Might Target:

- Access Protocols
- Acquisition Strategies
- Budget Estimates or Expenditures
- Confidential Documents
- Customer and Employee Data
- Hiring or Firing Strategies and Plans
- Investment Data
- Intellectual Property
- Innovation Capital
- Logistics
- Marketing Strategies
- Proprietary Formulas and Processes
- Negotiation Strategies
- Passwords
- Physical Security
- Pricing Strategies
- Proprietary Research, Formulas, and Processes
- Prototypes or Blueprints
- Supply Chain
- Technical Components and Plans

Intellectual Property Theft Incident:

Legal cases provide visibility into operational tactics, techniques, and procedures employed by threat actors seeking to violate the confidentiality of innovation capital.

In July, 2020, a federal grand jury returned an indictment charging two hackers, **Li Xiaoyu** and **Dong Jiazhi**, both trained in computer applications technologies at the same Chinese university, with hacking into the computer systems of hundreds of victims. The defendants probed for vulnerabilities in computer networks of companies developing COVID-19 vaccines, testing technology, and treatments.

Cyber Espionage Impact:

The Business Action to Stop Counterfeiting and Piracy (BASCAP), a business initiative organized by the International Chamber of Commerce, estimates the total value of counterfeit and pirated products is projected to **reach $1.9 to $2.8 trillion** in 2022.

Recommendation:

Establish a relationship with Information Sharing and Analysis Centers (ISACs). Join your respective ISAC for sector-based collaboration. ISACs collect, analyze and share actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.

Additionally, establishing a relationship with your local FBI field office will provide a valuable point-of-contact for a variety of information regarding potential incidents and events related to your security.