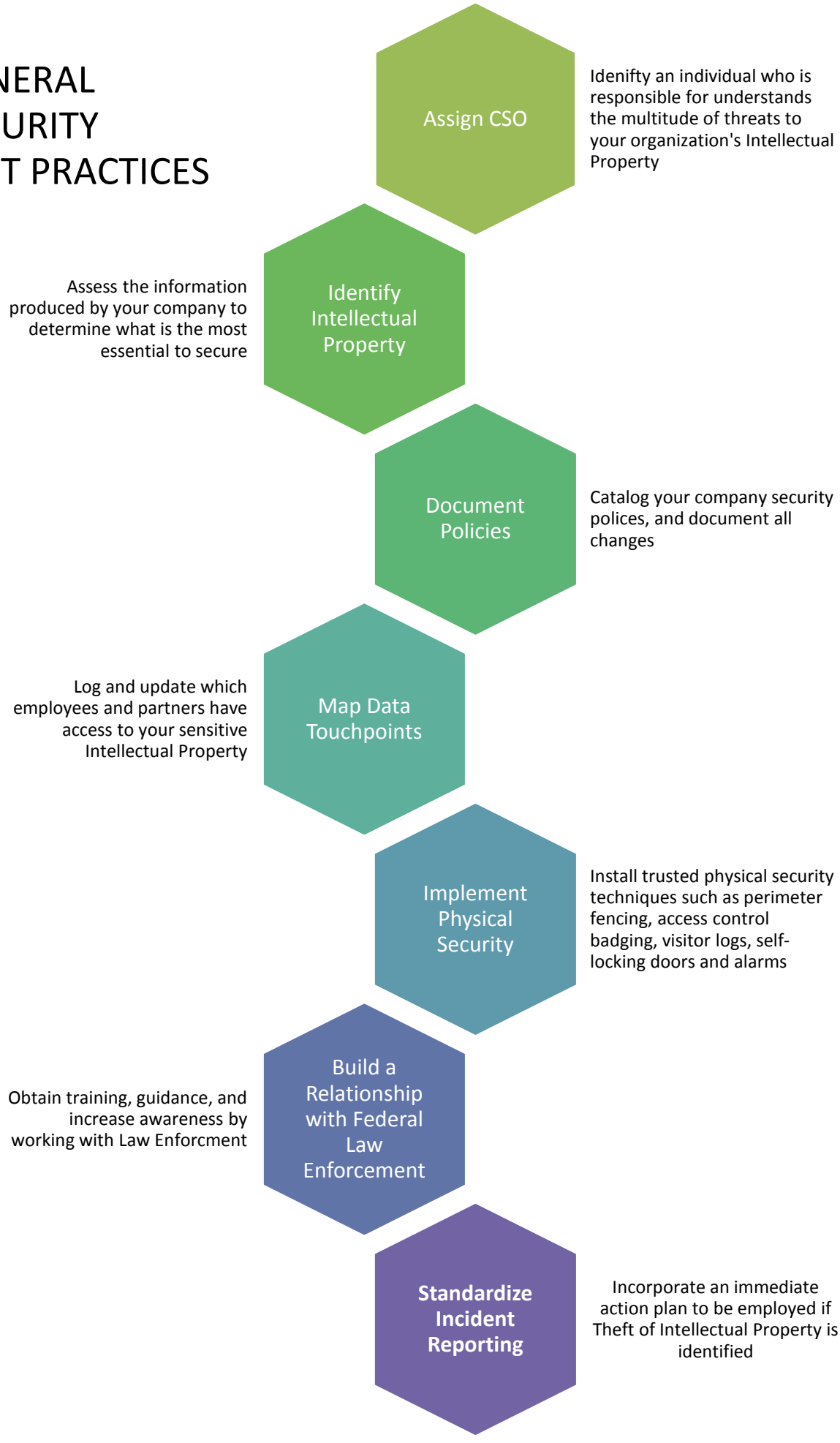
protect your startup

TIPS ON HOW TO SAFEGUARD YOUR COMPANY AND INTELLECTUAL PROPERTY

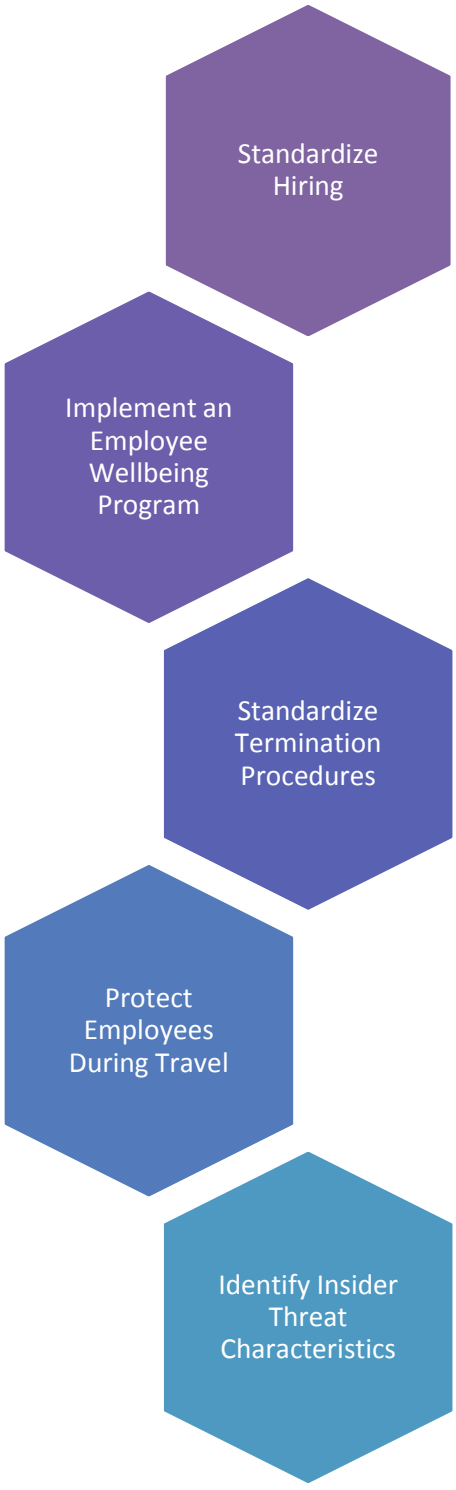
Office of Private Sector
Federal Bureau of Investigation

The information contained within this guide is intended to be used as a checklist for new organizations as they grow and work to protect their intellectual property (IP). **Disclaimer:** This document is a compendium of observed best practices. This document is not a recommendation of action from the U.S. Government. Adopting any of the practices herein is entirely at the discretion of the reader. Nothing herein comprises advice from the U.S. Government or any of its agents.

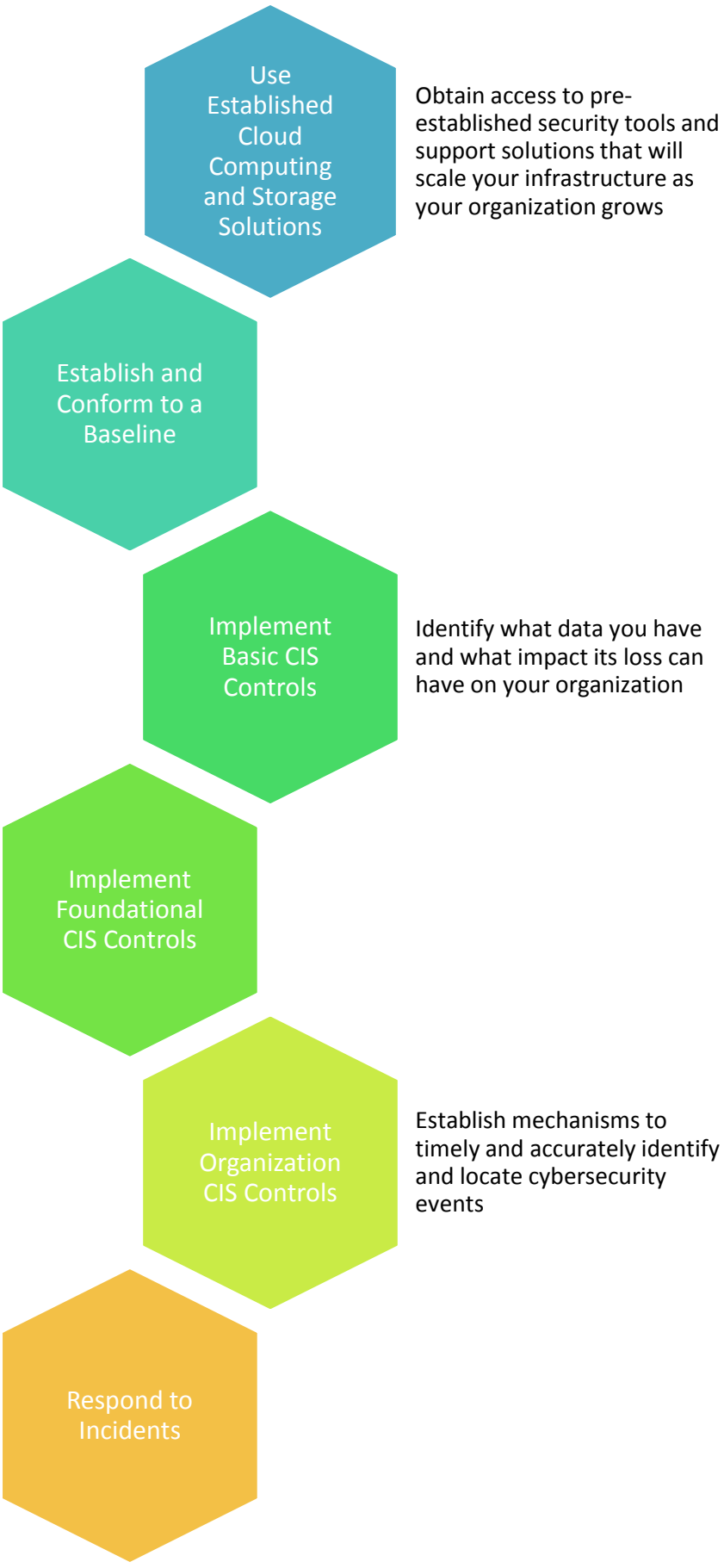
GENERAL SECURITY BEST PRACTICES



PERSONNEL SECURITY BEST PRACTICES



INFORMATION SECURITY BEST PRACTICES



ASSIGN A CHIEF SECURITY OFFICER

The Chief Security Officer (sometimes Chief Information Security Officer) is the single responsible executive for security in your organization. According to the Cyber Security Job Trends survey from Cybrary, only 49% of the 435 senior-level technology professionals polled reported that their company employs a full-time Chief Security Officer.

While hiring a full-time security officer may be a challenging financial burden for startups, one individual or group must be ultimately responsible for the security of the organization. This individual should be tasked with learning and understanding the myriad threats to the organization's Intellectual Property and be fully supported by the organization's leaders, HR, and legal elements.

- View a description of CISO responsibilities produced by the SANS Institute

IDENTIFY YOUR INTELLECTUAL PROPERTY

Completely protecting all of the information in your organization is a daunting prospect that is not always practical and can sometimes obstruct your ability to collaborate and grow. However, it is extremely important to identify the proprietary information held by your company that is most valuable and could cause damage to your business if disclosed to the public or a competitor. Understanding what this information is will allow you to apply the proper security measures to protect it, and restrict it to only those employees with a need to know. Note that your intellectual property may change as your company grows, so it is a good idea to review it regularly.

- The Legal Information Institute at Cornell has provided the legal definition of intellectual property here.

DOCUMENT POLICIES AND PROCEDURES

Properly documenting security policies and procedures and making them readily available to all personnel will allow you to formalize how your Intellectual Property is protected and how your employees use your systems. Ensure that you periodically review and update your security policies so they reflect your current business processes. If you do not protect your Intellectual Property, you will not receive legal redress if it is stolen.

- The SANS Institute maintains a list of security policies and associated templates for your organization to use

MAP DATA TOUCHPOINTS

Maintaining awareness of where your Intellectual Property is located and who has access to it allows you to build a complete picture of how you should protect your Intellectual Property. Ensure that you log, update, and clearly label both the digital and physical locations of your most sensitive Intellectual Property, and keep track of any partners that you provide your Intellectual Property to. This will also help you with post-

incident investigative efforts.

IMPLEMENT PHYSICAL SECURITY

Even basic physical security measures will help prevent theft of your Intellectual Property from burglaries and unauthorized visitors. Organizations should implement trusted physical security techniques such as perimeter fencing, visitor control systems, employee badging requirements, self-locking doors, and alarms.

- The Center for the Development of Security Excellence (CDSE) provides numerous resources in their Physical Security Toolkit

BUILD A RELATIONSHIP WITH FEDERAL LAW ENFORCEMENT

Building relationships with federal law enforcement can provide awareness and education on threats to your organization. Pre-establishing relationships with law enforcement may also increase the efficiency of incident responses.

- Each local FBI office maintains a Private Sector Coordinator who is in place to help local businesses collaborate with the FBI. Contact your local FBI office to learn more
- Once you have developed your security program, joining security groups such as Infragard or DSAC will allow you to stay up to date with the most current security issues and help you collaborate with like-minded security professionals

STANDARDIZE INCIDENT REPORTING

Incorporate an Incident Response Plan to be employed if theft of Intellectual Property is identified. This ensures that your employees understand their roles and have concrete instructions to follow in a stressful situation.

- This sample Incident Response Plan was created by Carnegie Melon University
- This checklist is provided to your organization by the FBI after an Intellectual Property theft incident is reported to ensure that your Intellectual Property was secured. Ensure that your organization will be able to answer all the questions on the checklist

STANDARDIZE HIRING

Implement a repeatable hiring process which identifies potential problem employees before they are brought onboard and helps to protect other employees who may be put in a difficult position because of their associations. Criminal checks, employment/education verifications, and security interviews are effective methods of screening applicants for employment, but most importantly you must get to know your employees.

- The University of Auckland has produced a short paper which discusses Counterproductive Workplace Behaviors and the impact they have on companies here

IMPLEMENT AN EMPLOYEE WELLBEING PROGRAM

Employee wellbeing programs will help increase organizational awareness about stressors that are adversely affecting your employees. These same programs will also give the organization an opportunity to intervene during periods of crisis for their employees, and help their employees mitigate stressors before they become unmanageable.

- The National Wellness Institute's Six Dimensions of Wellness Model provides some examples for employers to consider when setting up an Employee Wellbeing Programs
- The Harvard Business Review notes that Employee Wellbeing Programs often save companies a significant amount of money as well

IMPLEMENT EMPLOYEE TERMINATION PROCEDURES

Employees present a higher risk of stealing Intellectual Property in the period of time leading up to and directly after terminations, suspensions, or other discipline, particularly if the incident is contentious. Immediately upon termination and in some cases suspension, employees should have their network access and physical building access suspended and should have all company property confiscated. This will require collaboration and a unified effort between security, information technology, human resources, legal, and management.

- The Society for Human Resource Management has provided an example employee termination checklist

PROTECT EMPLOYEES AND Intellectual Property DURING TRAVEL

Always implement strict operational security measures while travelling, particularly to high threat countries. Many countries have introduced legislation which gives them the legal authority to take your Intellectual Property, with or without your knowledge. A few key items to remember:

- Use "burner" devices that do not have any information on them and can be destroyed upon return
- Do not use wi-fi
- Access your home network as little as possible, and only view documents in read-only mode
- Use a reputable VPN

- Review the Overseas Security Advisory Council alerts and updates before all travel

USE ESTABLISHED CLOUD COMPUTING AND STORAGE SOLUTIONS

Using a cloud-based development and data-storage environment gives your organization access to pre-established security tools and support solutions which will scale your infrastructure as your organization grows. Many of the information security best practices in this guide can safely be completed by service providers who have the resources and security functions in place to protect organizational data.

ESTABLISH A BASELINE

Ensure that all devices are set up with a standard security configuration using guidance from the vendor or an authoritative security publication such as the Center for Internet Security, whose principles of implementing basic, foundational, and organizational information security controls can help companies conceptualized and implement security. These provide gradual guidance for implementing security controls as your organization grows.

IMPLEMENT BASIC CIS CONTROLS

Begin to secure your information security posture by implementing CIS's Basic Controls. These basic controls will provide the foundation for good security practices, allowing you to map your assets and ensure that they are configured and maintained properly.

- Inventory and control hardware assets
- Inventory and control software assets
- Continuous vulnerability management
- Controlled use of administrator privileges
- Secure Configuration for hardware and software on mobile devices, laptops, workstations, and servers
- Maintenance, monitoring, and analysis of audit logs

IMPLEMENT FOUNDATIONAL CIS CONTROLS

Once your basic information security posture is completed, consider expanding your defensive capabilities, restricting access to appropriate systems, and actively monitoring what is going on in and around your network:

- E-mail and web browser protections

- Malware defenses
- Limitation and control of network ports, protocols, and servers
- Data recovery capabilities
- Secure configuration for network devices, such as firewalls, routers, and switches
- Boundary Defense
- Data Protection
- Controlled access based on the need to know
- Wireless access control
- Account monitoring and control

IMPLEMENT ORGANIZATIONAL CIS CONTROLS

Ensure that your entire organization is aware of information security requirements and actively look for vulnerabilities before they are exploited. This will allow you to stay ahead of threats and when they happen, mitigate them and restore your data:

- Implement a security awareness and training program
- Application software security
- Incident response and management
- Penetration tests and red team exercises
    - The Department of Homeland Security offers penetration testing services for interested organizations

RESPOND TO CYBERSECURITY EVENTS

Reduce the impact of cybersecurity events through following response plans and reporting to authorities:

- After a cybersecurity event:
    - Call the local FBI field office
    - Preserve original media as evidence (if not, make a forensic image)
    - Request your IT specialists conduct analysis from a copy instead of the original (if possible)
    - Gather all pertinent log files (DNS, Firewall, Proxy, System Event Logs)
    - Contact your ISP for additional logs and to provide filtering
    - Conduct a damage assessment (including damage valuation)
    - Many of these services can be provided by Cyber Incident Response Assistance (CIRA) accredited companies
- Resume normal operations after an event by:
    - Making full backups of critical business data/information
    - Regularly backing up all sensitive business data/information
    - Obtaining cyber insurance
    - Continually updating processes, procedures, and technologies

INSIDER THREAT CHARACTERISTIC ADDENDUM

These are some examples of suspicious activity that we have seen in recent years. If you see frequent, repetitive occurrences of the characteristics noted below, it may be helpful to give the FBI a call. Note that most insider threats will not fall cleanly into a single category; these categories are provided to help conceptualize common groups of characteristics. As your organization's security posture develops, it may be helpful to review some of the publicly available research on insider threats such as the Application of the Critical Path Method to Evaluate Insider Risks. Note that the FBI can direct you to additional resources when and if you need it.

General Characteristics:

- Any use of malware, rootkits, VPNs, or log manipulation to access or conceal access to large amounts of Intellectual Property
- Frequent, unexplained communication or association with foreign government officials, representatives of foreign companies, or foreign academics
- Unexplained or suspicious foreign travel
- Dishonesty or lack of candor regarding work products or use of organizational Intellectual Property
- Experiences significant stressors in their personal life such as financial hardship, failure of personal relationships, or legal problems
- Any significant, unexplained change in behavior

Steps an insider may take to steal Intellectual Property (adapted from Zonefox):

***Searching for sensitive Intellectual Property** –Conducting queries of organizational databases and networks for sensitive Intellectual Property which is outside the scope of their normal duties*
***Exploiting sensitive Intellectual Property** – Requesting access to sensitive Intellectual Property, attempting to increase their user privileges, or attempting to borrow, steal, or otherwise use another employee's credentials or elicit information from others*
***Acquiring sensitive Intellectual Property** – Taking sensitive Intellectual Property from a secure location and placing it on their local computer, desktop, or file folder*
***Exfiltrating sensitive Intellectual Property** – Taking sensitive Intellectual Property off of the organization's networks, through physical copies, e-mail, cloud storage solutions, websites, applications, etc.*

- *Due to the prevalence of encrypted means of communication, once an insider exfiltrates information it will be extremely difficult to track*

Trusted individuals can present significant risks to your organization if they decide to steal Intellectual Property. Insider threats may steal Intellectual Property for a variety of reasons, some of which may be malicious while others could be accidental or due to coercion. Recognizing the characteristics of insider threats can help an organization take action before their Intellectual Property is stolen. Potential examples of insider threats are:

EMPLOYEE COERCED THROUGH CONNECTIONS WITH AN AUTOCRATIC REGIME

A well-meaning employee whose family, friends, or assets are threatened by an autocratic regime who desires access to the Intellectual Property that they employee works on.

Example Characteristics:

- Have family, friends, property, or other attachments located in a country controlled by an autocratic regime

- The autocratic regime may threaten to hurt, take, or oppress whatever associations the employee has in the foreign country unless the employee steals their companies Intellectual Property and provides it to the regime. This puts the employee in an impossible position of choosing between their loved ones/personal assets or protecting their organization's Intellectual Property
- These employees may exhibit undue stress regarding their associations to the autocratic regime
- Other parts of their life, such as work or social life may suffer as a result of the stress

EMPLOYEE COERCED THROUGH HIGH-RISK ACTIVITY

An employee whose illegal, unethical, or otherwise risky behavior can be leveraged by a competitor or autocratic regime to blackmail them into providing their organization's Intellectual Property.

Example Characteristics:

- Typically have vulnerabilities in their lives which a competitor or autocratic regime may use to blackmail them
- May be characterized by poor decision-making and risk accepting behavior, such as:
    - Illegal or unethical activity
    - Substance abuse or misuse
    - Excessive debts or spending, or living beyond one's means
    - Extramarital affairs
    - Note that relationships with foreign nationals can also be exploited

MERCENARY

An employee who does not owe loyalty to a country or company, and will sell out to the highest bidder regardless of the legal or ethical consequences.

Example Characteristics:

- Often show signs of anti-social behavior (no conscience)
- Acts as though rules, instructions, and societal norms do not apply to them
- May have regularly broken rules, policies and laws in the past
- May be offered significant compensation in the form of job position, financial incentive, or property overseas
- May have significant issues in the workplace such as an inability to work with others, extreme disgruntlement, belligerence, and frequent violations of workplace rules and policies

ENTITLED EMPLOYEE[1]

An employee who has an extreme attachment to their work project or product to the extent that they feel they own it, and should be able to sell it to a competitor or autocratic regime. When the employee's personal, monetary, or egotistical expectations are not perceived as met by their organization, they may sell the Intellectual Property to an organization that provides them either the monetary reward or credit that they believe they deserve.

[1] Carnegie Melon's Guide to Insider Threats

Example Characteristics:

- Has experienced a dramatic professional setback such as a demotion, loss of position, or failure to advance which results in a significant grievance against the organization
- Moving away from a project or product may cause extreme duress, disgruntlement, and belligerence in the workplace
- May have significant issues in the workplace such as an inability to work with others, extreme disgruntlement, belligerence, and frequent violations of workplace rules and policies
- Exfiltration of data may be difficult to detect as this employee will likely already have personal copies of their work

AMBITIOUS LEADER[2]

An employee, often an organizational leader, who recognizes the value of the organization's Intellectual Property and takes the Intellectual Property with them to start their own company, or join another company they have a significant stake in.

Example Characteristics:

- Uses their position in an organization to gather Intellectual Property and market themselves to another company (or start their own)
- Leverages their position or relationship with others to target specific proprietary information or technology useful to another company they have a stake in, or potentially a foreign country that they have ties to

INFILTRATOR

An individual who has been directed by an autocratic regime to gain employment with/access to an organization specifically in order to steal their Intellectual Property.

Example Characteristics:

- These employees identify with and give ultimate loyalty to their country of origin (COO). Signs of this may include:
    - Use of "We" or "Us" when referring to a foreign country or company
    - Use of "Them" or "They" when referring to the US or employer
    - Desire to retire back to their COO
    - Returns to COO for significant life events
    - Maintains active political, cultural, or work associations with their COO
    - Has a job lined up in their COO
- May be significantly overqualified for their position or job role (such as an internship)
- Is often ideologically/politically motivated, and may legitimately believe that stealing Intellectual Property is their duty to their country. This means that they are often an effective, well-functioning individual without many of the vulnerabilities held by other insider threats

SUSPICIOUS VISITOR OR HOST

A foreign delegation or company representatives from an autocratic regime may attempt to steal your Intellectual Property during business meetings.

Example Characteristics and Items of Note:

- Presume at least one member of a delegation from a foreign regime is trained to steal your

[2] Carnegie Melon's Guide to Insider Threats

Intellectual Property

- When invited to a foreign country for business, US laws and protections no longer apply. Anything you take with you may be taken, examined, and potentially confiscated, overtly or without your knowledge
- Beware of excessive probing for information
- “Lost” visitors in restricted areas may be attempting to gather sensitive Intellectual Property
- Joint Ventures with or financing by Foreign Organizations is a growing vector of Intellectual Property Theft
- Be aware in the term sheet what Intellectual Property access you’re giving up, and insert clauses to protect your Intellectual Property
- Are you being asked to move production or management to a foreign jurisdiction?
- Note local law: often installing backdoors or giving up Intellectual Property is mandatory and not revealed to the company HQ; your employees may be coerced into providing access without your knowledge

NON-MALICIOUS

An employee, contractor, or business partner who accidentally discloses sensitive Intellectual Property may exhibit extreme carelessness, may not have been provided sufficient security training, or may be unclear on appropriate security measures.