Protecting and Defending Hidden Treasures

2021 Public-Private Analytic Exchange Program

Protecting Sensitive Data and Intellectual Property

Dangers of Foreign Travel

External & Insider Threats

Supply Chain Security & Integrity

Threats to Sensitive Data & Intellectual Property
# Table of Contents

Acknowledgement ........................................................................................................................................ ii

Executive Summary....................................................................................................................................... 1

An Introduction to Protecting Sensitive Data and Intellectual Property...................................................... 2

Dangers of Foreign Travel ............................................................................................................................. 5

Insider Threat ................................................................................................................................................ 7

External Threats ............................................................................................................................................ 9

Supply Chain Security and Integrity ............................................................................................................ 11

Conclusion ................................................................................................................................................... 13

Further Reading .......................................................................................................................................... 14

DISCLAIMER STATEMENT ............................................................................................................................ 15
Acknowledgement

We acknowledge and thank the federal government agencies, companies, academia, and other organizations that supported the development of this paper. We also thank the Office of the Director of National Intelligence (ODNI) and the U.S. Department of Homeland Security (DHS) for the opportunity to have participated in the 2021 Public-Private Analytic Exchange Program (AEP).

2021 AEP Public-Private Team Members – Protecting Sensitive Data and Intellectual Property

- Lee Kim, JD, CISSP, CIPP/US
- Amy Weschler, Delta Air Lines
- Chris Chamberlin, U.S. Department of Homeland Security
- Dr. Brian Gant, Maryville University
- Sean Dospoy, Walgreens
- Stephen Streng, University of Minnesota

People and Organizations Consulted

We are grateful to the following individuals who provided information and expertise for this report:

- Brian Dahlin, University of Minnesota
- Christian Terry, Delta Air Lines
- Craig Byrkit - Internal Security / Insurance Industry
- David Makous, Esq., Lee, Hong, Degerman, Kang & Waimey PC
- Germán Castro, International SOS
- Nitin Natarajan, Cybersecurity and Infrastructure Security Agency
- Mangoné Fall, Cleveland Clinic
- Merritt Baer, Amazon
- Michael Scobee, Delta Air Lines
- Roland Corvington, Financial Industry
- Von Welch, University of Indiana
Executive Summary

Virtually all organizations have sensitive data and intellectual property of some kind. Both are intangible assets that enhance the bottom line of every organization. Indeed, certain organizations depend upon the safeguarding of sensitive data and intellectual property in order to function. Sensitive data can be any kind of information that requires some sort of enhanced protection (e.g., classified information, confidential business information, privileged information, etc.). Intellectual property is defined by law and deals with information that essentially is a creation of the mind. Intellectual property includes, but is not limited to, copyrights, patents, trademarks, and trade secrets.

Thus, sensitive data and intellectual property must be protected using appropriate administrative, technical, and physical safeguards. Knowing what to do is only half the battle. Implementing best practices and mitigating risk are also necessary to adequately protect the information. Risks to sensitive data and intellectual property include the following: (1) dangers of foreign travel, (2) insider threat, (3) attack from external threat actors, and (4) supply chain integrity and security. While this list is non-exhaustive, these represent common scenarios in many organizations. A range of topics will be discussed along these lines, including basic fundamentals, advanced techniques, and know-how.
An Introduction to Protecting Sensitive Data and Intellectual Property

Every organization needs to protect its sensitive data and intellectual property. Both sensitive data and intellectual property have value to each organization and need to be safeguarded with enhanced measures.

Intellectual property is defined by laws that give the owner (i.e., the rights holder) certain rights. “Intellectual property” refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.¹ The rights associated with intellectual property include copyrights, patents, trademarks, and trade secrets. Intellectual property may also include computer programs that are developed in house and research discoveries, among other things. Examples of intellectual property include proprietary databases, software interfaces, computer programs, chemical compositions, pharmaceutical formulations, pictorial graphic and sculptural works, novel and non-obvious methods and apparatuses, manuscripts, documentation, musical compositions, sound recordings, and the like.

Simply put, intellectual property laws protect intellectual property. Intellectual property rights stem from the intellectual property laws, which may vary in accordance with the jurisdiction. For example, computer programs may be protected by copyrights (including the right to reproduce, distribute, and modify). A claimed invention in an issued patent may be protected by applicable patent laws. Trade secret laws may protect secret formulas, methods, processes, as may be applicable.

In the United States, copyrights and patents are protected by Federal law. Trade secrets may be protected by state and Federal law. Copyright registration with the US Copyright Office is required in order to have standing to sue for copyright infringement in Federal court. Patents are issued by the United States Patent and Trademark Office (USPTO) after examination of the application and a determination by the USPTO that a patent should be granted based upon the examination of the application. Laws in other countries may vary. Although intellectual property treaties set forth a minimum standard of protection, there may be variation in the implementation of such intellectual property laws—and, not all countries are signatories to these various treaties.

“Sensitive data” is defined as any information that may require enhanced protection.² Sensitive data may include confidential commercial, financial, proprietary information, and other privileged information. Sensitive data, if improperly disclosed, may cause harm to the owner of the sensitive data, the subject of the sensitive data, and/or give a competitor an unfair advantage. Sensitive data could, for example, include classified information, proprietary information, identifying information about an individual, or personally identifiable information (PII).³ A leak or breach of sensitive data may cause reputational and financial harm to the organization that acts as the custodian and/or for the subject of the information.
Examples of intellectual property:

- Manuscripts
- Computer programs
- Pictorial, graphic, and sculptural works
- Music compositions and sound recordings
- Secret formulations
- Chemical compositions
- Certain apparatuses, methods, processes, or systems
- Secret client lists

Examples of sensitive data:

- Credit card information
- Protected health information
- Corporate finances
- Employee information
- Privileged information
- Classified information
- Information not appropriate for disclosure or use by third parties
- Cyber threat indicators and defensive measures for cybersecurity purposes

Identifying sensitive data and intellectual property are key initial steps. You cannot protect what you do not know you have. Sensitive data and intellectual property may include a wide range of information. Thus, it is helpful to inventory the information that constitutes sensitive data and intellectual property. Throughout the information lifecycle, such information needs to be regularly identified, protected, and, if appropriate, destroyed at the end of the lifecycle.

Intellectual property and sensitive data must be safeguarded with appropriate administrative, physical, and technical controls and safeguards. Intellectual property and sensitive data should be protected to safeguard the reputation of the organization and the organization’s goodwill with its customers and stakeholders. Additionally, the use and disclosure of intellectual property and sensitive data may be subject to legal agreements such as non-disclosure agreements. Non-disclosure agreements may be unilateral (one way exchange of confidential information) or mutual (each party being a receiving party and a disclosing party of confidential information). Confidential information, as defined by non-disclosure agreements, may be broadly defined and the agreed upon scope is subject to negotiations between the parties to the agreement.

Administrative safeguards include policies, procedures, plans, practices, training, and agreements relating to the protection of intellectual property and sensitive data. Policies and procedures should be created in light of the organization’s mission and priorities, as well its relative risk posture. The less risk the organization is willing to accept, the more the controls should be stringent. To that end, the foundation of any security program is the risk
assessment. Comprehensive risk assessments should be conducted or reviewed at least once a year, if not more frequently.

Policies and procedures should also be reviewed at least once a year in light of the results of the risk assessment. Procedures should be reviewed to ensure that they are consistent with the policies. Actual practices should also be reviewed to make sure that they are aligned with the policies and procedures—if they are not in alignment, then this may indicate the need to revisit the policies and procedures and/or retrain staff to comply with the existing policies and procedures. Further, if there are many exceptions that have been granted to the written policies and procedures, this may also indicate the need to revisit the policies and procedures that are in place and/or retrain staff, as appropriate. A security program is not effective if there are too many exceptions. Inconsistently applied controls and safeguards may potentially lead to significant vulnerabilities that can be ripe for exploitation.

In addition to a comprehensive risk assessment, a robust identity management program is also essential. Role-based access should be granted as appropriate and accounts should be timely provisioned and de-provisioned in a timely manner. Zero trust technology solutions may also be implemented across the enterprise to secure access across applications, devices, systems, and networks. Products, services, vendors, consultants, and employees also need to be carefully selected and vetted to mitigate risks.

While non-exhaustive, key risks to sensitive data and intellectual property for many organizations include the following: (1) dangers of foreign travel, (2) insider threat, (3) attack from external threat actors, and (4) supply chain security and integrity. However, in spite of these risks, there are ways to mitigate them. Best practices for mitigating risks to sensitive data and intellectual property include the following:

- Identify and inventory your sensitive data and intellectual property, whether it is in physical form, electronic form, or otherwise
- Understand who has access to which data, for what purpose, and when
- Establish data retention and data destruction policies for such information
- For especially sensitive data or intellectual property such as trade secrets, keep a log of who has access to the specific information
- Ensure that people, processes, and technologies are in alignment and that appropriate administrative, physical, and technical safeguards are in place; and
- Regularly evaluate, test, and train on the policies, procedures, and safeguards that are in place.
Dangers of Foreign Travel

Traveling abroad, whether for personal or business travel, poses an increased risk to your and/or your company’s sensitive data and intellectual property. For business travelers, the sensitive data and intellectual property that need to be protected will vary depending upon the organization. However, business travelers and personal/leisure travelers also have to consider protecting their own personally identifiable information (PII). According to NIST, PII is information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. Examples include personal and business calendar information, account information, and/or financial information.

Experts across various sectors agree that one of the biggest issues facing international travelers is simply being cognizant of the potential risks that may impact their well-being or their organizational data integrity. The best way to mitigate that risk is to be aware of the risk profile and do everything you can to minimize exposure. The risk profile is the combination of those factors which may cause others to target you or your organization based on their perception, values and goals.

The first consideration when preparing to travel is to be cognizant that you will be traveling to a foreign country where culture, traditions, and perceptions might possibly be different from one’s home country. Be sure to self-reflect and be cognizant of the danger of “mirror imaging,” or assuming that others perceive and process information in the same manner as you do through personal experience. “Mirror imaging” may lead you to believe that you are not a high-profile target based on your perception of yourself and your worth, while others may absolutely view you as a high-profile target. Accordingly, it is important for you to familiarize yourself with the foreign country’s culture, traditions, and perceptions before you leave for that country. An equally important step is to be sure to familiarize yourself with the foreign country’s legal and constitutional framework. Rights and requirements in one country may be entirely different in another.

Additionally, monitoring the geo-political stability and relationship between your home country and country of destination is critical. Ongoing tensions between the home country and country of destination may or may not be apparent. However, such dynamics may lead to you being a higher value target. Thus, you may be a prime target for surveillance, cybercrime, and enhanced monitoring with the risk of possible detention by the foreign government. Accordingly, foreign governments may choose to legally collect your data during routine customs processing or during any other government encounters which may result in sensitive data and intellectual property being compromised.

It is important to minimize sensitive data and intellectual property that can either be disclosed or derived. It is important, if possible, to travel with laptop, phone, and other computing devices that either have minimal amounts of such information or even a loaner, burner, or other disposable device without any such information.
Upon arrival at your destination, best practices are to refrain from connecting any device to public WiFi networks, lock unattended devices, ensure your communications are encrypted prior to sending and while in transit, and ensure that data is encrypted while at rest. Strong authentication should be used for your accounts.

Additionally, public USB charging stations pose a significant risk to sensitive data and intellectual property. A hack known as “juice jacking” is becoming more common. A threat actor can install malware within a charging kiosk and have a payload that either automatically downloads your data once connected via USB, or otherwise installs malware onto your device. Accordingly, it is not recommended to charge your device at the airport or another place where you are not familiar with the particular charging equipment. It is not unusual for certain “cheap” devices to have pre-loaded malware—thus, the danger of plugging into something you are not familiar with.

On another note, do not assume that devices which you leave in your hotel room are guaranteed to be safe. A general recommendation is to always take your devices with you. Your laptop, mobile phone, and other devices may not be safe in the hotel safe, since hotel personnel may have a master code to the hotel safe and may surreptitiously gain access.

Another thing to keep in mind when you are traveling is that if you lose control of your laptop or device for more than a trivial amount of time, you have to assume that your laptop or device may have been compromised. There may also be circumstances in which you may be forced to give up control of your laptop or device, such as going through airport security or when attempting to cross a country’s borders, and other scenarios. These are reasons why it is critical for laptops and devices that you are traveling with do not contain sensitive data or intellectual property, if at all possible.

Once your travel is complete, be sure to follow your company’s policy in regard to any loaner, burner, or disposable device. If you traveled with a personal or corporate laptop or device, be sure to work with your IT department to ensure that a full wipe is performed and that a clean installation of operating system and software is done—if that laptop or device is to be reused.

The following are proactive measures that you can undertake to help mitigate the dangers of foreign travel:

- Familiarize yourself with the foreign country’s culture, traditions, perceptions, as well as its legal and constitutional framework before you leave for that country
- Monitor the geo-political stability and relationship between your home country and country of destination
- Travel with burner, loaner, or disposable devices, preferably, or with a device with the absolute minimum amount of sensitive data and/or intellectual property
- Do not use public USB charging stations
- Refrain from connecting any device to public WiFi networks
- Secure unattended devices
Ensure your data is encrypted in transit and at rest; ensure that your communication channels are also encrypted

Use strong passwords for your accounts; and

Once your travel is complete, be sure to follow your company’s policy in regard to any loaner, burner, or disposable device.

Insider Threat

Within any organization, insiders may pose a significant threat to the confidentiality and integrity of sensitive data and intellectual property. According to the Cybersecurity and Infrastructure Security Agency (CISA), an insider is defined as “any person who has or had authorized access to or knowledge of an organization’s resources, including personnel, facilities, information, equipment, networks, and systems.” An insider does not necessarily need to have physical access, nor does the individual have to be physically on the premises. Further, an insider has the potential to harm an organization, whether maliciously or negligently. CISA defines insider threat as “the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the [organization’s] mission, resources, personnel, facilities, information, equipment, networks, or systems.” Note, however, that an insider only needs to have trusted access.

The damage from insider threat activity can often be greater than the damage caused by external threat actors. The US Center for Development of Security Excellence (CDSE) notes that “trusted insiders may commit malicious acts, such as fraud, theft, sabotage, espionage, unauthorized disclosure, workplace violence, and more,” while “unwitting insiders may inadvertently disclose sensitive data, unknowingly download malware, or facilitate other cybersecurity events.” No organization is immune to insider threat; thus, it is critical that organizations develop insider threat mitigation programs.

The first step to any such mitigation program is recognizing key indicators of insider threat and educating employees on the importance of recognizing and reporting suspicious incidents or behavior. Key indicators for insider threat include, but are not limited to, work performance, foreign connections, criminal, violent, or abusive conduct, financial status, substance abuse and addictive behaviors, and psychological conditions. Insider threat actors may be motivated by extremist ideology, affiliation with malicious state actors, financial stress (e.g., debt) or opportunity, sense of disgruntlement, or other life stressors or may be unwittingly manipulated by outside individuals through tactics such as social engineering or phishing attempts. Accordingly, it is essential for employees, contractors, and other staff to be carefully selected and vetted prior to on boarding, and also during the course of their employment with the organization.

On a related note, training employees and contractors to recognize potential risk indicators and report suspicious activity helps to mitigate the risk of insider threat activity. Ideally, organizations should have reporting channels for suspicious activity and security awareness training for insider threat. Employees, contractors, and other staff should be educated on how to recognize and report suspicious activity. This could involve formal online reporting,
anonymous hotlines, or other appropriate internal information sharing with either supervisors or other designated points of contact (such as human resources).

When developing an insider threat program, formal policies and procedures should be created and regularly reviewed. Also, organizations should identify who has access to what information and why, adopt a risk-based approach for classifying the sensitivity of data, information, and intellectual property, and implement appropriate access controls and safeguards. Vendors, consultants, and others should be given special consideration regarding their access to intellectual property and/or sensitive data. Stakeholders across the organization should have input on how to effectively manage and mitigate insider threats, including IT, legal, human resources, and other mission critical departments. Effective and timely communication are the keys to success of any insider threat program. Alignment of actual practices with the formal policies and procedures for insider threat is also key.

Consider the following scenario: an investment firm employed a systems administrator and IT security engineer. The organization notified the employee that he made a critical mistake in reconfiguring a system and did not follow the appropriate notification protocols which caused massive production delays. As a result, it was decided that his contract would not continue and that, by the end of the day, his station should be cleared. From the time of this notification to the end of the day, the employee scripted a logic bomb to erase all data on certain servers, including the backup copies. The malicious script was designed to lay dormant for two months. After the employee left the organization, the replacement employee noticed some irregularities in the system only a couple days after the previous employee had left. The firm was able to remove the logic bomb and the former employee was found, arrested and charged. This case illustrates the need for a strict and seamless process for the removal, reassignment, and/or termination of employees. In terms of best practices, employee accounts should be immediately frozen or otherwise de-provisioned before employees are notified that they have been terminated. A physical escort should be utilized to remove the employee from the work area, and an exit interview should be conducted at that time.

Organizations should be proactive in their approach to mitigating insider threat. Best practices for mitigating insider threat include the following:

- Developing a formal risk-based insider threat policy and program
- Aligning practices with policies and procedures
- Understanding risk indicators for insider threat
- Carefully selecting and vetting employees, contractors, vendors, consultants, and others
- Educating employees on recognizing and reporting suspicious activity
- Ensuring a culture of appropriate information sharing within the organization
- Establishing clear processes for reporting, investigating, and responding to potential insider threat activity
o Knowing what’s normal and what’s not normal in terms of employee or contractor working hours, behavior, and activity, as well as normal behavior and activity for users, systems, and networks
o Investing in new technologies to combat insider threats, such as Security Incident and Event Management (SIEM) software/programs and User Entity Behavior Analysis (UEBA) programs
o Collaborating and communicating with stakeholders across the organization on effectively managing and mitigating insider threats, including IT, legal, human resources, and other mission critical departments
o Developing operational procedures that limit unintentional exposure to protected information, such as restricting use of public sharing or collaboration platforms without vetted security controls and safeguards; and
o Reviewing policies annually as well as immediately following any occurrence of insider threat activity (especially if significant).

**External Threats**

External threats originate from external threat actors. External threat actors are those wanting to cause harm who are outside of an organization. These are individuals or entities that are not insiders and do not have trusted access to the organization. External threat actors may include cybercriminals, hacktivists, cyber-terrorists, and script kiddies.

Further, external threat actors do not merely exist in the cyber realm. An authorized individual (such as an employee) may be let into a secure building, but an unauthorized individual may “tail” that individual by striking up conversation or making it look like he or she is with that individual—thus (potentially) bypassing any security controls in place. Once within the organization, the individual can potentially steal or otherwise compromise information—especially if the corporate culture is not one of “see something, say something.”

Cybercriminals may also target intellectual property for the purpose of intellectual property theft, such as information on patentable inventions and trade secrets. Further, cybercriminals may work with nation state actors to help nation state actors carry out politically motivated goals and objectives.

Cybercriminals target organizations often for financial gain. Motivations and objectives may vary. However, cybercriminals may steal sensitive data such as personally identifiable information for the purpose of identity theft. Such information may be resold on the black market. Various means for doing so include, but are not limited to, ransomware and other malware. Because many organizations have flat (i.e., unsegmented) networks that do not restrict access across the network, it is fairly easy for cybercriminals to laterally move throughout networks and gain information.
However, cyber espionage occurs domestically as well. In such instances, entities may hire cybercriminals to do their bidding in order to steal sensitive data and/or intellectual property of a competitor.

The organizations that cybercriminals target span all sectors. Although companies in the financial, retail, and energy industries, healthcare organizations, academic and research institutions, and local governments have been prominently victimized, no organization is immune. Often, many organizations are vulnerable to the same or substantially similar cyber attacks.

Hacktivists typically hack into systems and networks for sociological or ideological reasons or causes. The level of sophistication of the hacktivists versus the defensive skills of those who are defenders often results in an asymmetric threat to the organization. The technical skill of a hacktivist may be quite high, but unfortunately the technical skill of a cybersecurity defender is not always of the same level.

Notwithstanding the foregoing, script kiddies are individuals who may not have a very high level of skill, but deploy exploits that are essentially pre-made (formulated by someone else, such as a proof of concept). Public and free exploits are routinely developed and distributed for known vulnerabilities in software and operating systems. Furthermore, free and automated exploit tools, like Metasploit or Cobalt Strike, can be used to execute various attacks on systems and networks.

On a related note, the primary means by which cybercriminals, script kiddies, hacktivists, and others infiltrate systems is by way of phishing. The reason is that the weakest link of any cybersecurity program tends to be people. People can be fooled or otherwise deceived, especially with sophisticated phishing techniques. Thus, a best practice when receiving a suspicious email is to verify the sender’s request or communication whenever possible using an out of band channel (e.g., telephone or a virtual or physical meeting).

Concerns about phishing attacks are at all time highs. Compounding this problem, attackers are also leveraging technology, such as deepfakes and other synthetic identities to simulate a person’s likeness or voice. In light of this ever-evolving threat, organizations must stay one step ahead and develop protocols to combat threats today and into the future.10

Best practices for mitigating external threats include the following:

- Ensuring that defense-in-depth is adhered to and that appropriate administrative, technical, and physical safeguards are in place
- Carefully selecting and vetting vendors, consultants, and others that provide products and services, devices, service providers, and the like
- Regularly conducting and reviewing comprehensive end-to-end security risk assessments and proactively managing risk
- Enabling multi-factor authentication and complex passwords
Deploying a robust identity management program, including in regard to privileged accounts and regular accounts
Deploying endpoint detection and response (EDR) solutions
Implementing a robust security awareness program, including in regard to phishing and good cyber hygiene
Timely provisioning and de-provisioning of user accounts, including for employees, contractors, and others
Ensuring that role-based access for each user is tailored appropriately, as roles may change over time
Determining a baseline for normal user, system, and network behavior and activities and understanding when abnormal behavior and activities are occurring
Ensuring that intellectual property and sensitive data are not publicly accessible, including by way of cloud and/or exposed end points
Implementing advanced technology for detecting and identifying threats (e.g., leveraging artificial intelligence)
Implementing zero trust technology to secure access across applications, devices, systems, and networks
Blocking and tackling security incidents in a timely manner
Having robust incident response policies and procedures, including as to internal and external points of contact
Ensuring a culture of appropriate information sharing within the organization and with external partners
Ensuring that data is regularly backed up and that backups are accessible, if restoration of data is required; and
After an incident occurs, taking note of any lessons learned, conducting a gap analysis, and implementing any proactive steps in an attempt to prevent the incident from recurring in the future.

Supply Chain Security and Integrity

Supply chains are increasingly at risk that are critical to energy, food, financial, IT, and other infrastructure. Supply chains include the systems, collection, and connection of resources (e.g., human, material, financial, information, etc.) that are used to create a product or service. Supply chains are often vast in size and instantaneous in terms of responsiveness. Any given supply chain likely includes multiple partners and/or service providers, each of which potentially contains their own multi-faceted layers of partners. It is the responsibility of organizational leaders to fully assess supply chains to ensure potential risks are identified and mitigated in a timely manner.

An information supply chain involves information flows through computer technology hardware, software, and devices used to deliver a service. Examples of the information supply chain are found in all critical infrastructure sectors, including financial services, energy, healthcare and public health, and transportation systems. Recent managed service provider attacks have highlighted the risk from our information technology supply chain.
Managed service providers increase the attack surface of the companies that use them. The compromise of one managed service provider may put many of its clients at risk. This is true for small, medium, and large organizations. Essentially, every organization is a potential target.

According to the NIST Glossary of Information Security Terms, Supply Chain Risk Management (SCRM) is defined as “the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of product and service supply chains.” As applied to information systems, SCRM refers to the process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes the following: (1) conducting a risk assessment; (2) implementing a risk mitigation strategy; and (3) employing techniques and procedures for the continuous monitoring of the security state of the information system.

Notwithstanding the foregoing, there are proactive steps that every organization can do to help mitigate risks to supply chain security and integrity. This applies to both the companies that are supplying the products and services, as well as the organizations that procure such products and services.

Best practices for mitigating supply chain security and integrity risks include the following:

- Adopting and following the NIST Cyber Supply Chain Risk Management Framework (C-SCRM), which provides guidance on activities necessary to manage cybersecurity risk associated with external parties.
- Adopting and following the NIST Risk Management Framework (RMF) and/or the Cybersecurity and Infrastructure Agency’s (CISA’s) Supply Chain Risk Management Essentials; these guidelines are applicable to both computer-based information and intellectual property that might not be in digital form.
- Ensuring appropriate selection and vetting of third-party vendors, including analyzing where they get their components and subcomponents, as well as how they mitigate potential insider threat.
- Ensuring vendor contract language specifies requirements and expectations for supply chain security and integrity.
- Incorporating zero trust principles – do not trust and always verify.
- Actively managing all enterprise assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments for monitoring and protection; and
- Actively managing all software on the network so that only authorized software is installed and can execute.
Conclusion

It is vitally important to adequately manage and mitigate risks to sensitive data and intellectual property, taking into account the dangers of foreign travel, insider threat, external threats, and supply chain integrity and security. Most of these risks can be managed through preparedness, planning, prevention, and training. However, when incidents do occur, they must be mitigated and the root cause must be ultimately identified. Valuable lessons can be learned as a result of the incidents that do occur. Additionally, if incidents recur, this is a clear sign that certain gaps exist that must be addressed. Organizations need to be resilient, not just simply recover from the incident.

Sensitive data and intellectual property are the lifeblood of virtually every organization. These intangible assets, too, are the hidden treasures of our organizations. But, we need to know where they are, who has access to them, and how to secure them in order to safeguard them from compromise (e.g., data leaks, breaches, etc.). While it may take more effort, an ounce of prevention is worth a pound of cure. The damage to an organization that can result in light of the unauthorized disclosure and use of intellectual property and sensitive data can be immense—and this is something that must be avoided at all costs.

Keys to successfully managing and mitigating risks to intellectual property and sensitive data include regularly conducting and reviewing comprehensive risk assessments and applying appropriate administrative, physical, and technical controls and safeguards. Additionally, actual practices need to be aligned with policies and procedures, as well as the mission and priorities of the organization.
Further Reading


DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.