The following documents listed below have been compiled from our exhaustive list of Cyber Incident Response and Reporting Program (CIRRP) packets for purposes of providing an overview of the depth and details of the material we've developed.

For additional samples, please email us at info@flank.org

# List of Risks, Threats, Attacks, and Related Incidents & Events

For [company name] to be able to adequately respond to cybersecurity occurrences, all users (i.e., employees, contractors, vendors, guests, etc.) need to be aware of the following risks, threats, attacks, and related incidents that can cause significant damage to organizational assets:

- **Cyber Intrusion:** The unauthorized act of spying, surveilling, and the possible theft of information and/or damage to information systems.
- **Ransomware:** A type of malicious software that essentially blocks access to the victim's data or threatens to publish or delete it until a ransom is paid
- **Malware:** An umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software
- **Watering Hole:** A computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. The malware used in these attacks typically collects information on the user.
- **Phishing:** The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords, credit card numbers, Personally Identifiable Information (PII), and other data deemed sensitive and confidential.
- **Spoofing Attack:** An event in which one person or program successfully masquerades as another by falsifying data, thereby gaining an illegitimate advantage.
- **Web Application Development Security Risks:** These are risk associated with developing software used for web facing systems, such as e-commerce servers, publicly accessible servers that provide general content, and other forms of information that are "public" facing within the untrusted Internet. Learn more at https://www.owasp.org about such threats.
- **Denial of Service (DoS) Attack:** A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
- **Distributed Denial of Service (DDoS):** A type of a type of Denial of Service Attack (DoS) where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack
- **Credential Reuse:** A cyber incident whereby account credentials are leaked from one website, and because users often use the exact same or similar passwords on multiple websites, those accounts are then also compromised.
- **Deliberate, Unauthorized Access Attempts:** Abuse by an individual to gain access to a system by continuing to enter a username and password until they are effectively locked out or ultimately denied.
- **Session Hijacking and Man-in-the-Middle (MITM) Attacks:** The exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer. Simply stated, any attack that involves the exploitation of a session between devices is session hijacking, with the "session" being a connection between devices in which there is state.

- **Hacktivism:** The subversive use of computers and computer networks to promote a political agenda
- **Drone Jacking:** The hijacking of a drone, either by physically capturing the device or by compromising its navigation system.
- **Social Engineering:** The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purpose
- **Insider Threats:** A malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems
- **Acceptable Use Violations:** Violating an organization's usage rights to information systems.
- **Loss or Theft of Assets:** Assets (such as physical assets, along with data and information) that is either physically or electronically lost or stolen.
- **Loss of Sensitive Data:** The loss (i.e., theft or unauthorized use) of data, which includes, but is not limited to the following: Protected Health Information (PHI), Personally Identifiable Information (PII), Personally Identifiable Financial Information (PIFI), cardholder data, and other types of data deemed personal/confidential, etc.
- **Rogue Software:** A form of malicious software and Internet fraud that misleads users into believing there is a virus on their computer, and manipulates them into paying money for a fake malware removal tool (that actually introduces malware to the computer). It is a form of scareware that manipulates users through fear, and a form of ransomware.
- **Drive-by-Downloads:** The unintentional download of a virus or malicious software (malware) onto your system. A drive-by attack will usually take advantage of (or "exploit") a browser, app, or operating system that is out of date and has a security flaw.
- **Malvertizing:** The use of online advertising to spread malware by injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
- **Advanced Persistent Threats:** A network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.
- **Other:** Any other risk, threat, attack, and related incident not discussed in the above listed descriptions.

**Risks, Threats, Attacks, and Related Incidents & Events Matrix**

| Risks, Threats, Attacks, and Related Incidents | Tools/Solutions in Place | Responsible Party | Contact Information |
|---|---|---|---|
| Cyber Intrusion | | | |
| Ransomware | | | |
| Malware | | | |
| Watering Hole | | | |
| Phishing | | | |
| Spoofing Attack<br>Web Application Development Security Risk | | | |
| Denial of Service (DoS) Attack | | | |
| Distributed Denial of Service (DDoS) | | | |
| Credential Reuse | | | |
| Deliberate, Unauthorized Access Attempts | | | |
| Session Hijacking and Man-in-the-Middle (MITM) Attacks | | | |
| Hacktivism | | | |
| Drone Jacking | | | |

| | | | |
|---|---|---|---|
| **Social Engineering** | | | |
| **Insider Threats** | | | |
| **Acceptable Use Violations** | | | |
| **Loss or Theft of Assets** | | | |
| **Loss of Sensitive Data** | | | |
| **Rogue Software** | | | |
| **Drive-by-Downloads** | | | |
| **Malvertizing** | | | |
| **Advanced Persistent Threats** | | | |
| **Other** | | | |

## Incident Analysis and Response

Analyzing a risk or threat to determine if it is in fact an incident/or could become an incident, requires authorized personnel to conduct preliminary assessments, such as profiling, being knowledgeable about normal, baseline behaviors, and any deviations from such baselines, along with other necessary measures. Any incident deemed to be a threat to the organization requires a rapid response from authorized personnel, such as the IRT personnel. This rapid response will follow a standard course of action designed to minimize the impact of the incident to the organization's critical network and system infrastructure.

**Technical Impact Analysis**

Assessing the technical impact of a given incident is a critical element for helping to understand the overall severity of the given incident and what systems, if any, have been affected. As such, authorized personnel are to assess the following issues and documenting their findings within the Incident Response Submission Form (IRSF):

- What systems have been affected, both directly and indirectly, by the incident?
- Did the incident result in any type of a breach of sensitive/confidential data, such as PII, etc.?
- What security systems were bypassed/not-effective in stopping the breach?
- Was the incident detected early enough to allow for adequate response mechanisms to be put into place?
- From a quantitative perspective, exactly what many systems were affected, both directly and indirectly, by the incident?
- What type of access was utilized by the attackers in penetrating [company name]'s systems?

**Business Impact Analysis**

Assessing the business impact of a given incident is also a critical element for helping to understand the overall severity of the given incident and what people, places, and operations, if any, have been affected. As such, authorized personnel are to assess the following issues and documenting their findings within the Incident Response Submission Form (IRSF):

- What impact has the incident had on the ability to continue operations?
- Has the incident resulted in any type of danger to immediate [company name] personnel or the general public at-large?
- Has the incident resulted in a breach of internal accounting/financial and/or any other type of highly sensitive/confidential [company name] information?
- Does the incident require [company name] to find and retain external, third-party resources for assistance?

**Incident Rating Levels and Impact**

IRT personnel are to formally assume control and to identify the threat and its severity to the organization's information systems. Specifically, the following levels are to be used for determining severity and the overall impact of the incident:

- **LOW:** There is a MINIMAL impact on the organization from this incident. Examples include, but are not limited to, the following: email spam, moderate, limited, and/or minimal attack on the network, [please provide other examples specific to your organization].
- **MEDIUM:** There is a SIGNIFICANT impact on the organization from this incident. Examples include, but are not limited to, the following: short-term system downtime, attacks on the network that result in "any" type, but not "significant", breach of records/assets, [please provide other examples specific to your organization].
- **HIGH:** There is a SERIOUS impact on the organization from this incident. Examples include, but are not limited to, the following: threat of life, significant physical destruction, distributed denial of service (DDoS)/network attack that brings down/paralyses the network in terms of "Confidentiality, Integrity, and Availability", significant breach of customer specific Personally Identifiable Information (PII), ransomware attack where significant records/assets have been seized/compromised, [please provide other examples specific to your organization].

IRT personnel are to also determine (as best as possible during the early stages of the incident) what recovery efforts, if any, are to be implemented for fully recovering from an incident. Specifically, the following categories are to be used for determining recovery initiatives:

- **Regular:** Recovery time is predictable.
- **Extended:** Recovery time is unpredictable as additional resources are necessary.
- **Not Recoverable:** Recovery is not possible, thus additional initiatives are to be undertaken.

**NCCIC Descriptions**

If the above levels and corresponding information are deemed insufficient – thus, the organization is seeking a more comprehensive list of reporting schema – then [company name] is to use the following category descriptions provided by the National Cybersecurity and Communications Integration Center (NCCIC) Scoring System:

- **Functional Impact:** A measure of the actual, ongoing impact to the organization.
- **Observed Activity:** What is known about threat actor activity on the network.
- **Location of Observed Activity:** Where the observed activity was detected in the network.
- **Actor Characterization:** Attributing an incident to a particular actor set and understanding the skill levels and intentions of that actor.
- **Information Impact:** Used to describe the type of information lost, compromised, or corrupted.
- **Recoverability:** The scope of resources needed to recover from the incident.
- **Cross-Sector Dependency:** A weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA).
- **Potential Impact:** Estimates the overall national impact resulting from a total loss of service from the affected entity.

**Documentation**

Documentation is imperative for incident response practices, thus authorized IRT personnel are to officially open an incident response ticket via completion of [name of ticketing system] provided for such measures. All information contained within the ticket is to include the required fields from the **Incident Response Submission Form (IRSF).** Alternatively, the IRSF can be uploaded and attached to the actual ticket that was opened by IRT personnel. Because the severity of incident can vary, it is understandable that many times the first and most important task will be to immediately contain the incident, and then subsequently complete the applicable form.

**Notification (Internal)**

Notifying all relevant personnel and parties, both internally and externally, is critical to [company name]'s overall incident response and reporting initiatives. The ability to assign tasks, keep individuals informed, while continuing

to communicate on the progress of response mechanisms put in place is essential. The following external personnel are to be notified regarding incidents against [company name]'s network.

**Incident Response Notification Matrix (internal)**

| Name and Contact Information | Title | Reporting Requirements | Communication Method |
|---|---|---|---|
| ? | President & CEO | Provide high-level information regarding the incident and what initiatives are being put in place to quarantine the issue and resolution for ultimately removing the incident. | Choose an item. |
| ? | CIO | | Choose an item. |
| ? | CTO | | Choose an item. |
| ? | CISO | | Choose an item. |
| ? | Human Resources | | Choose an item. |
| ? | ? | | Choose an item. |
| ? | ? | | Choose an item. |
| ? | ? | | Choose an item. |

**Notification (U.S. Department of Defense) for DoD Contractors**

In accordance with the DoD's **DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal** (https://dibnet.dod.mil/portal/intranet/Splashpage), DoD contractors shall report as much of the following information as can be obtained to the DoD within 72 hours of discovery of any cyber incident.

1. Company name
2. Company point of contact information (address, position, telephone, email)
3. Data Universal Numbering System (DUNS) Number
4. Contract number(s) or other type of agreement affected or potentially affected
5. Contracting Officer or other type of agreement point of contact (address, position, telephone, email)
6. USG Program Manager point of contact (address, position, telephone, email)
7. Contract or other type of agreement clearance level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
8. Facility CAGE code
9. Facility Clearance Level (Unclassified, Confidential, Secret, Top Secret, Not applicable)
10. Impact to Covered Defense Information
11. Ability to provide operationally critical support
12. Date incident discovered
13. Location(s) of compromise
14. Incident location CAGE code
15. DoD programs, platforms or systems involved
16. Type of compromise (unauthorized access, unauthorized release (includes inadvertent release), unknown, not applicable)

17. Description of technique or method used in cyber incident
18. Incident outcome (successful compromise, failed attempt, unknown)
19. Incident/Compromise narrative
20. Any additional information