PICNIC™

HUMAN ATTACK SURFACE PROTECTION (HASP) FRAMEWORK

June 2023 | v1.0

The HASP Framework arms the cybersecurity community with best practices aligned to NIST CSF and MITRE ATT&CK that proactively protect the human attack surface

Cyber defenders across all critical infrastructure sectors lack a holistic and comprehensive cybersecurity framework that specifically helps them manage at scale the risks associated with OSINT and social engineering. Such a framework is necessitated, however, by the fact that the majority of breaches continue to be the result of exposed data and the human element. With threat actors now having the capability to leverage AI, the effectiveness and scale of these human-centric attacks is increasing to unprecedented levels.

HASP is a unique framework developed by Picnic in collaboration with cybersecurity experts worldwide that reduces the risk of human-centric attacks involving social engineering and OSINT exploitations. This framework, aligned with NIST CSF and MITRE ATT&CK, helps cyber defenders tackle social engineering risk at the source using best practices that proactively reduce the human attack surface.

By leveraging HASP's insights and guidance, organizations can better protect themselves and their employees from the devastating impacts of attacks that exploit the human element, resulting in an improved overall security posture, more focused intelligence, a lower number of active threats, less attention fatigue at the SOC, and reduced cybersecurity operational expenses. The HASP framework is freely available to individuals and organizations. Start building a stronger defense with HASP today.

All contributions and feedback are appreciated. To contribute to the HASP Framework, please contact us at haspframework@getpicnic.com.

Contributors

The following cybersecurity experts are the founding contributors to v1.0 of the HASP Framework.

Jim Routh
Former CSO and CISO

Rachel Tobac
CEO
SocialProof Security

Rob Lee
CEO & Founder
Dragos

Lt. Gen. Charles Moore Jr.
Deputy Commander, U.S. Cyber Command
U.S. Air Force (ret.)

Christopher Key
Former CPO
Mandiant

Niloofar Razi Howe
Cybersecurity Strategist and Executive

Ben Fried
Former CIO
Google

Jessica Brooks
VP Cybersecurity Compliance
Goldman Sachs

Frank Catucci
CTO & Head of Security Research
Invicti Security

Jonathan Cran
Product & Engineering Leader
Google

Vice Admiral TJ White
Commander of Fleet Cyber Command, 10th Fleet, and Navy Space Command
U.S. Navy (ret.)

Matt Polak
Founder & CEO
Picnic

Henry Ristuccia
Former GRC Leader
Deloitte

Mark Ford
Former National Risk and Financial Advisory Sector Leader, Higher Education
Deloitte

Nandita Bery
Director, InfoSec
Equinix

Scott Goodhart
CISO Emeritus
AES

Christine Schaefer
CMO
CrashPlan

Jason Nations
Director of Enterprise Security
OGE Energy Corp.

Major General Ed Wilson
Former DASD for Cyber Policy
U.S. Department of Defense (ret.)

Jim Somborovich
Cybersecurity Leader & Veteran (USMC)

Parag Baxi
Former VP, Product
Picnic

Manit Sahib
Former Director, Global Threat Intelligence
Picnic

Risk Categories & Mitigation Actions

1. High Risk Employees

1.1 — Identify high value employee targets

Typical Owner: Identity Access Management Team (IDAM)
MITRE Alignment: T1589
NIST CSF Alignment: ID.RA-1

High-value employee targets refer to employees who have access to sensitive data, intellectual property, or critical systems that, if compromised, could result in significant harm to the organization. These employees are often targeted by malicious actors seeking to gain unauthorized access to sensitive information or systems.

Examples of high value employee targets include, but are not limited to:

- Executives and extended executive staff such as assistants and chiefs of staff
- Board members who have access to sensitive strategic information and decision-making processes
- IT and OT staff with privileged access to sensitive systems and data
- Employees who manage critical infrastructure or production systems
- Finance and accounting staff who have access to financial records and payment systems
- 3rd party vendor management employees who work with and manage outside parties
- Legal staff who handle sensitive legal documents and communications
- Sales and marketing staff who have access to customer data and business strategy information
- Human resources staff who handle sensitive employee data and company policies
- Research and development staff who work on proprietary technology or intellectual property
- Public relations and communications staff who manage company-controlled social media accounts and messaging
- Customer support staff who have access to customer data and communication channels
- Corporate development staff involved in M&A
- Government relations staff who have access to critical company strategy documents
- Corporate strategy, competitive intelligence, and market research staff who often have sensitive information about company plans

It is important to consider the context and unique risks within each organization when identifying high-value employee targets. This may include roles that are critical to the business or have access to sensitive data or systems specific to the organization's industry or operations. A thorough risk assessment should be conducted to identify all high-value employee targets for the organization. Once identified, specific procedures should be established and implemented to ensure these employees are adequately protected from social engineering attacks and other targeted threats. Additionally, increased detection and monitoring measures should be implemented for high-value employee targets, and their threat intelligence should be correlated to provide elevated monitoring and protection. Enrolling high-risk employees in an elevated threat monitoring program can also help to mitigate risks associated with insider threats.

1. High Risk Employees

1.2 — Identify highly accessible employee targets

Typical Owner: Identity Access Managment Team (IDAM)
MITRE Alignment: T1589
NIST CSF Alignment: ID.RA-1

Highly accessible employee targets are individuals who are vulnerable to social engineering attacks due to their personality traits, behaviors, and online profiles. These employees tend to be more open, trusting, and willing to engage with others, which makes them attractive targets for attackers who use social engineering techniques to gain unauthorized access to sensitive information.

Examples of highly accessible employee targets include individuals who volunteer, give philanthropically, teach, mentor, or coach. These employees are often well-known in their communities and may have a public presence, which makes it easier for attackers to gather information about them and craft targeted attacks. This also includes brand ambassadors such as PR professionals, community outreach personnel, and thought leaders.

In addition, highly accessible employees are often active on social media platforms and may share personal information that can be used to gain access to sensitive data. For example, an attacker could use information shared on social media to craft a convincing phishing email that appears to be from a trusted source.

Note that while high-value employees are relatively easy to identify using traditional corporate markers, highly accessible employees can be more difficult for organizations to identify since the markers are nearly entirely outside of the corporate information sphere.

1. High Risk Employees

1.3 — Conduct social engineering risk assessments for high value employee targets

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: M1047
NIST CSF Alignment: ID.RA-5

Conducting social engineering risk assessments for high value employee targets is an important step in identifying potential vulnerabilities and mitigating the risk of insider threats. Social engineering is a technique used by attackers to manipulate individuals into divulging confidential information, performing actions, or providing access to systems or data. High value employee targets are more likely to be targeted by these types of attacks due to their access to sensitive information or systems and, as a result, can become unwitting insider threats.

To conduct a social engineering risk assessment for high value employee targets, the organization should start by identifying the potential attack vectors and techniques that could be used against these individuals. This may involve researching known attack methods and tactics used by threat actors targeting similar organizations or conducting simulated social engineering attacks to identify potential vulnerabilities.

Once potential attack vectors and techniques have been identified, the organization should assess the current security controls in place for high value employee targets and determine any gaps or weaknesses. This may include reviewing access controls, monitoring and detection capabilities, security awareness training, and incident response procedures.

The next step is to develop and implement a plan to address any identified vulnerabilities and improve security controls. This may involve implementing additional security awareness training for high value employee targets, enhancing access controls and monitoring, and developing incident response procedures specifically tailored to these individuals.

Overall, conducting social engineering risk assessments for high value employee targets is an important part of a comprehensive insider threat program. By identifying potential vulnerabilities and implementing appropriate security controls, organizations can reduce the risk of insider threats and protect their sensitive data and systems.

1. High Risk Employees

1.4 — Conduct social engineering risk assessments for highly accessible employee targets

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: M1047
NIST CSF Alignment: ID.RA-5

Conducting social engineering risk assessments for highly accessible employee targets is important because they are more vulnerable to social engineering attacks due to their high visibility, open communication style, and extensive online presence. Attackers can use information from public sources, such as social media, to craft convincing phishing emails, impersonate trusted contacts, or gather personal information to use for future attacks.

To conduct a social engineering risk assessment for highly accessible employee targets, the organization should first identify who those employees are based on the criteria previously established. The organization can then use a variety of techniques to assess their susceptibility to social engineering attacks, such as simulated phishing campaigns, targeted information gathering exercises, and social media monitoring.

Simulated phishing campaigns involve sending fake phishing emails to employees to test their awareness and response to phishing attempts. The results can help identify employees who are more likely to fall for phishing attacks and may require additional training or monitoring. Targeted information gathering exercises involve gathering publicly available information about employees to determine their susceptibility to social engineering attacks and identify potential weaknesses in their personal and professional profiles.

Social media monitoring involves monitoring the social media activity of employees to detect any suspicious behavior or interactions that could indicate a social engineering attack. This can be done manually or through the use of automated tools that can flag unusual activity or keywords.

By conducting social engineering risk assessments for highly accessible employee targets, organizations can better understand the unique risks these employees face and take steps to mitigate those risks through targeted training and awareness campaigns, increased monitoring, and other security measures.

1. High Risk Employees

1.5 — Establish and implement procedures for high value employee targets

Typical Owner: GRC (Governance Risk and Compliance) Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-7

Establishing and implementing procedures for high value employee targets is crucial to protecting them and the organization from targeted attacks. The procedures should outline specific steps and protocols for handling sensitive information and potential security threats.

Here are some reasons why it is important to establish and implement procedures for high value employee targets:

- Mitigating Risks: Establishing procedures can help mitigate the risks associated with high value employee targets. Procedures should outline how sensitive information is handled, who has access to it, and what steps should be taken if an attack is suspected or occurs.
- Standardization: Having standardized procedures in place ensures that all employees are aware of the risks and the steps that should be taken to protect themselves and the organization. This can help to prevent confusion or misunderstandings that could lead to security breaches.
- Compliance: Depending on the industry, there may be regulations or standards that require organizations to have specific procedures in place to protect sensitive information or individuals. Establishing and implementing procedures can help ensure compliance with these regulations.
- Demonstrating Commitment: By establishing procedures, organizations can demonstrate their commitment to protecting the security and privacy of their employees and sensitive information. This can help to build trust with stakeholders and customers.

To establish and implement procedures for high value employee targets, the following steps can be taken:

- Conduct a Risk Assessment: Before establishing procedures, it is important to conduct a risk assessment to identify the specific risks faced by high value employee targets. This can include vulnerabilities in physical security, information security, and social engineering.
- Establish Procedures: Based on the results of the risk assessment, procedures should be developed that address the identified risks. This can include protocols for handling sensitive information, access controls, and reporting procedures.
- Communicate Procedures: Once procedures are established, they should be communicated to all relevant employees. This can include training sessions, email communications, or inclusion in employee handbooks.
- Monitor and Update Procedures: Procedures should be regularly monitored and updated as necessary to ensure that they remain effective in mitigating the risks faced by high value employee targets.

By following these steps, organizations can establish and implement procedures that help to protect their high value employee targets and the sensitive information they handle.

1. High Risk Employees

1.6 — Establish and implement procedures for highly accessible employee targets

Typical Owner: GRC (Governance Risk and Compliance) Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-7

Establishing and implementing procedures for highly accessible employee targets is important to mitigate the risks associated with their vulnerability to social engineering attacks. Social engineering attackers often target these individuals because of their openness and willingness to engage with others, making them more susceptible to manipulation or coercion.

To establish and implement procedures for highly accessible employee targets, organizations can consider the following steps:

- Identify the highly accessible employee targets: Conduct a risk assessment to identify the individuals in the organization who are highly accessible based on their personality, behaviors, and profile.
- Educate employees: Provide training to employees on social engineering attacks and the risks associated with them. This can include identifying phishing emails, suspicious phone calls, or unsolicited requests for personal or company information.
- Implement access controls: Limit the access of highly accessible employee targets to sensitive information or systems. For example, these individuals may not need access to all customer data or financial records.
- Implement monitoring and detection systems: Implement systems to detect and monitor unusual activity or behavior related to highly accessible employee targets. This can include monitoring of social media accounts or communication channels.
- Establish incident response procedures: Develop procedures to respond to incidents related to social engineering attacks against highly accessible employee targets. This can include procedures for reporting incidents, investigation, and response.

By establishing and implementing these procedures, organizations can help mitigate the risks associated with social engineering attacks against highly accessible employee targets. It is important to regularly review and update these procedures as new risks and threats emerge.

1. High Risk Employees

1.7 — Increase detection and monitoring for high value employee targets

Typical Owner: SOC
MITRE Alignment: M1040
NIST CSF Alignment: DE.CM-3

Increasing detection and monitoring for high value employee targets is crucial in protecting an organization from social engineering attacks. This is because high value employees are often targeted by cyber criminals due to their access to sensitive information and critical systems within the organization. By increasing detection and monitoring, an organization can quickly identify and respond to potential social engineering attacks targeting these employees.

To increase detection and monitoring for high value employee targets, an organization can implement the following measures:

- Implementing access controls: Limiting access to sensitive systems and data to only those who need it can reduce the likelihood of social engineering attacks. This can include using multi-factor authentication, role-based access control, and monitoring of access logs.
- User awareness training: Providing regular training and awareness programs to high value employees can help them identify and respond to social engineering attacks. This can include training on phishing emails, pretexting, and other common tactics used by attackers.
- Regular testing: Conducting regular phishing tests and social engineering simulations can help identify areas of vulnerability within the organization and allow for targeted improvements to be made.
- Monitoring of network activity: Regular monitoring of network activity can help identify potential attacks targeting high value employees. This can include monitoring for unusual login activity, unauthorized access attempts, and abnormal data transfers.
- Incident response planning: Developing a clear incident response plan that includes procedures for responding to social engineering attacks targeting high value employees can help minimize the impact of an attack and allow for a quicker response.

By implementing these measures, an organization can improve its ability to detect and respond to social engineering attacks targeting high value employees.

1. High Risk Employees

1.8 — Increase detection and monitoring for highly accessible employee targets

Typical Owner: SOC
MITRE Alignment: M1040
NIST CSF Alignment: DE.CM-3

Increasing detection and monitoring for highly accessible employee targets is important because they may be more vulnerable to social engineering attacks due to their public profiles and activities. By monitoring their behavior and communications, an organization can detect and prevent attempts to exploit their openness and willingness to engage with others.

To increase detection and monitoring for highly accessible employee targets, the organization can implement several measures:

- Implement a social media monitoring program: By monitoring the social media activity of highly accessible employees, the organization can detect any suspicious activity or attempts to gather information.
- Conduct regular security awareness training: Highly accessible employees should be provided with regular training on social engineering techniques and how to identify and respond to suspicious activity.
- Implement strict access controls: Access to sensitive information and systems should be restricted only to those who need it, and strict procedures should be implemented for granting access.
- Use technology solutions: The organization can implement technologies such as intrusion detection systems, firewalls, and email filters to detect and prevent social engineering attacks.
- Conduct regular risk assessments: Regular risk assessments should be conducted to identify any new threats or vulnerabilities that may affect highly accessible employee targets.

By implementing these measures, the organization can increase its ability to detect and prevent social engineering attacks against highly accessible employee targets.

1. High Risk Employees

1.9 — Correlate threat intelligence with high risk employees

Typical Owner: Threat Intel
MITRE Alignment: M1019
NIST CSF Alignment: ID.RA-5

Correlating threat intelligence with high-risk employees can help organizations identify potential threats and take proactive measures to mitigate them. By monitoring external sources of threat intelligence, such as known threat actor groups or new attack techniques, and correlating that information with employee data, organizations can identify employees who may be at higher risk of being targeted by social engineering attacks.

One way to correlate threat intelligence with high-risk employees is to establish a threat intelligence program that aggregates and analyzes external sources of intelligence. This program should be designed to identify emerging threats, vulnerabilities, and attack methods, and to provide actionable intelligence to security teams.

The program can be supported by various tools, such as threat intelligence feeds, open-source intelligence gathering, and dark web monitoring. These tools can help to identify potential risks, such as phishing campaigns targeting specific employees or groups within the organization.

Once the threat intelligence program is established, the organization can begin correlating the threat intelligence with employee data to identify high-risk employees. This process may involve identifying employees who work in critical or sensitive roles, as well as those who have a high public profile or are highly active on social media.

By identifying high-risk employees, the organization can then take appropriate steps to mitigate the risk of social engineering attacks. This may include targeted security awareness training, increased monitoring and detection, and the implementation of additional security controls, such as two-factor authentication or access restrictions.

Overall, correlating threat intelligence with high-risk employees is an important part of an effective security strategy. By identifying and mitigating potential risks, organizations can reduce the likelihood of successful social engineering attacks and better protect their sensitive data and assets.

1. High Risk Employees

1.10 — Enroll high risk employees in elevated threat monitoring program

Typical Owner: Insider Risk Team
MITRE Alignment: M1017
NIST CSF Alignment: PR.IP-7

Enrolling high-risk employees in an elevated threat monitoring program is crucial for protecting the organization against social engineering attacks. High-risk employees, including those who hold sensitive positions or are highly accessible, are often targeted by attackers who use various techniques to gain access to the organization's systems and data.

An elevated threat monitoring program provides an additional layer of protection for high-risk employees by monitoring their activities, both online and offline, and detecting any suspicious behavior or potential threats. This allows for a timely response to any incidents or attacks, minimizing the potential damage to the organization.

To enroll high-risk employees in an elevated threat monitoring program, the organization should first identify all employees who meet the criteria for high-risk status. This includes those in sensitive positions or who are highly accessible, as well as those who have been identified as targets in previous attacks.

The organization should then work with a security vendor or internal security team to implement the elevated threat monitoring program. This may include deploying specialized monitoring tools that track employee activity and behavior, as well as conducting regular risk assessments and providing targeted security training to high-risk employees.

It is also important to establish clear guidelines and procedures for responding to potential threats or incidents identified through the monitoring program. This includes outlining the roles and responsibilities of key stakeholders, such as the security team, human resources, and management, and establishing protocols for communication and incident response.

Overall, enrolling high-risk employees in an elevated threat monitoring program is a critical step in protecting the organization from social engineering attacks. By identifying and monitoring potential threats, the organization can proactively respond to incidents and minimize the potential impact on the organization's systems and data.

2. Exposed Employee PII

2.1 — Identify exposed employee PII

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1589
NIST CSF Alignment: ID.RA-2

Identifying exposed employee personally identifiable information (PII) in the public domain is important for protecting the privacy and security of employees. If employee PII is publicly available, it can be used by attackers to launch social engineering attacks and gain unauthorized access to corporate systems and data. Additionally, if employee PII becomes exposed in a data breach, on data broker sites, or through some other means, employees may be at risk of identity theft and other forms of fraud.

To identify exposed employee PII in the public domain, organizations can conduct regular scans of publicly available information sources such as social media, online forums, and data breach repositories. These scans can be performed manually or through the use of automated tools that can identify and flag potentially exposed information.

Once exposed employee PII has been identified, organizations should take steps to remove the information from public sources and notify affected employees of the exposure. In addition, employees should be trained on the risks of exposing their own PII online and how to properly secure their personal information.

Overall, identifying and mitigating exposed employee PII in the public domain is an important aspect of a comprehensive cybersecurity program that seeks to protect both the organization and its employees from the risks of cyber attacks and identity theft.

2. Exposed Employee PII

2.2 — Reduce exposed employee PII

Typical Owner: Security Awareness Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-7

Reducing exposed employee personally identifiable information (PII) in the public domain is an essential step in protecting high-risk employees from social engineering attacks. Social engineers often use publicly available information to create targeted attacks against employees, making it crucial to minimize the amount of exposed employee PII in the public domain.

To reduce exposed employee PII in the public domain, organizations can take the following steps:

- Conduct regular web searches for employee PII: Organizations can use online search tools to look for employee information that is available in the public domain. This includes searching for employee names, email addresses, phone numbers, and other identifying information.
- Remove or minimize unnecessary PII: Organizations can work with employees to identify any publicly available PII that can be removed or minimized. For example, employees can be advised to remove personal information from their social media profiles or limit the amount of personal information they share online. Also, request the removal of personal information from data brokerages.
- Monitor for new exposures: Organizations can use automated tools to monitor for new employee PII exposures in the public domain. This can include monitoring for employee PII on data broker sites, social media, online directories, and other public websites. This process should be done continuously.
- Implement a data privacy policy: Organizations can implement a data privacy policy that outlines the types of employee information that should not be shared publicly. This policy can include guidelines for employees to follow when creating online profiles or communicating online.
- Educate employees: Organizations can educate employees on the importance of protecting their personal information and the potential risks associated with sharing personal information online. This education can include training sessions, awareness campaigns, and regular reminders to employees.

By taking these steps, organizations can minimize the amount of employee PII available in the public domain and reduce the risk of social engineering attacks against high-risk employees.

3. Exposed Credentials

3.1 — Identify exposed work credentials

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1589.001
NIST CSF Alignment: ID.RA-2

Identifying exposed work credentials in the public domain is important because these credentials can be used by cybercriminals to gain unauthorized access to company systems and sensitive data. Exposed credentials can be found on various websites, including pastebin and underground forums, as well as through phishing attacks that target employees.

To identify exposed work credentials in the public domain, the organization can use various tools and techniques such as:

- Credential monitoring services: These services can monitor the dark web and other sources for leaked credentials and alert the organization if any employee credentials are found.
- Regular searches: The organization can periodically search for exposed credentials on public websites, such as pastebin or underground forums.
- Phishing simulations: The organization can conduct phishing simulations to test employee awareness and identify any employees who fall for phishing attacks, which may result in exposed credentials.
- Employee training: The organization can provide regular training to employees on how to recognize and report phishing attempts and the importance of strong password management.

Once the exposed work credentials have been identified, the organization should take immediate steps to mitigate the risk, such as:

- Resetting affected passwords: Employees whose credentials have been exposed should be required to reset their passwords immediately.
- Multi-factor authentication: The organization should implement multi-factor authentication for all systems and applications to reduce the risk of unauthorized access.
- Monitoring for suspicious activity: The organization should monitor for any suspicious activity related to the exposed credentials and take appropriate action if any unauthorized access is detected.
- Regular password changes: The organization should require employees to regularly change their passwords to reduce the risk of exposed credentials being used in the future.

By identifying and mitigating exposed work credentials in the public domain, the organization can significantly reduce the risk of cyber attacks and data breaches.

3. Exposed Credentials

3.2 — Identify exposed personal credentials

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1589.001
NIST CSF Alignment: ID.RA-2

It is important for organizations to identify exposed personal credentials in the public domain to prevent their employees from becoming victims of credential stuffing attacks or other forms of cyberattacks that can compromise their personal accounts. Credential stuffing is a type of attack where attackers use automated tools to try username and password combinations on various online services using credentials stolen from other data breaches. If an employee's personal account is compromised, it can lead to the attacker gaining access to their work-related accounts, especially if the employee uses the same password across multiple accounts.

To identify exposed personal credentials in the public domain, organizations can use various tools and techniques. One common approach is to use a dark web monitoring service that scans the dark web and other public domains for exposed credentials. These services can also alert organizations when an employee's personal information is found in a data breach. Additionally, organizations can encourage their employees to use password managers that generate and store strong, unique passwords for each online account.

Another way to identify exposed personal credentials is to train employees on how to recognize phishing emails and other types of social engineering attacks that can lead to the theft of personal information. Employees should also be encouraged to use multi-factor authentication (MFA) wherever possible to add an extra layer of security to their personal accounts.

Overall, by identifying exposed personal credentials in the public domain, organizations can take proactive steps to protect their employees from cyberattacks and minimize the risk of a data breach.

3. Exposed Credentials

3.3 — Identify exposed service credentials

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1078
NIST CSF Alignment: ID.RA-2

Identifying exposed service account credentials in the public domain is important for organizations to prevent unauthorized access to critical systems and data. Service accounts are used to automate tasks and provide system-level access, which makes them valuable targets for attackers. If service account credentials are exposed in the public domain, attackers can use them to gain access to the targeted system, potentially causing significant damage.

To identify exposed service account credentials in the public domain, organizations can use a variety of methods such as:

- Regularly conducting web searches using the names of the organization's service accounts to identify any exposed credentials on public websites or forums.
- Monitoring dark web marketplaces and forums for the sale or trade of service account credentials.
- Setting up alerts with threat intelligence feeds to receive notifications when service account credentials are found on the internet.

Once exposed service account credentials are identified, it is important to promptly reset them and implement additional security measures to prevent future exposures. This may include implementing two-factor authentication for service accounts, restricting access to critical systems, and increasing monitoring and detection capabilities for unusual behavior.

3. Exposed Credentials

3.4 — Empower employees to mitigate risk through credential management

Typical Owner: Security Awareness Team
MITRE Alignment: M1027
NIST CSF Alignment: PR.AC-1

Empowering employees to mitigate risk through credential management is essential for reducing the risk of a social engineering attack. By providing employees with the tools and knowledge to manage their credentials effectively, they can take an active role in protecting their own information and the information of the organization.

There are several ways that an organization can empower employees to manage their credentials effectively:

- Educate employees on password best practices, such as using complex and unique passwords for each account, avoiding the use of easily guessable personal information, and not sharing passwords with others.
- Provide employees with password managers or other tools to help them manage their credentials securely.
- Implement multi-factor authentication (MFA) for all accounts, which requires a user to provide more than one form of authentication to access an account. This can include something they know (like a password), something they have (like a security token), or something they are (like a fingerprint).
- Encourage employees to report any suspicious activity or potential security breaches, such as phishing attempts or unauthorized access to their accounts.
- Regularly remind employees to update their passwords and review their account activity to ensure that there is no unauthorized access.

By empowering employees to manage their credentials effectively, organizations can reduce the risk of a social engineering attack and better protect their sensitive information.

3. Exposed Credentials

3.5 — Reset passwords of currently-set exposed credentials

Typical Owner: Identity Access Management Team (IDAM)
MITRE Alignment: M1027
NIST CSF Alignment: PR.AC-1

Your organization should reset passwords of currently-set exposed credentials to prevent unauthorized access to sensitive information or systems. If an employee's credentials have been compromised and are exposed in the public domain, an attacker may use them to gain access to your organization's systems and data.

To reset passwords of currently-set exposed credentials, your organization can follow these steps:

- Use a tool or service that scans the internet for exposed credentials associated with your organization's email domain or employees' usernames.
- Identify the exposed credentials that are currently set and active.
- Notify the affected employees to change their passwords immediately and advise them on creating strong and unique passwords.
- Ensure service will not be interrupted by disabling or resetting exposed credentials.
- Disable the exposed credentials to prevent any further use of them by unauthorized individuals.
- Monitor for any suspicious activity related to the exposed credentials and take appropriate action if any is detected.

Your organization should also consider implementing multi-factor authentication (MFA) as an additional layer of security to protect against credential-based attacks. MFA requires an additional form of verification, such as a code sent to a mobile device or biometric authentication, in addition to a password to gain access to systems or data.

3. Exposed Credentials

3.6 — Block work, personal, and service exposed credentials from reuse

Typical Owner: Identity Access Management Team (IDAM)
MITRE Alignment: M1027
NIST CSF Alignment: PR.AC-1

Blocking exposed credentials from reuse is important to prevent unauthorized access to company systems and data. Attackers often use exposed credentials to gain access to other accounts, so it is critical to block the reuse of these credentials.

Organizations may prevent the reuse of compromised login credentials by implementing password policies that draw from both personal and work-related data breaches, and mandate the creation of unique and robust passwords for every account. Additionally, organizations can use tools such as password managers to generate and store complex passwords.

Multi-factor authentication (MFA) can also be implemented to add an additional layer of security to accounts. MFA requires users to provide additional information beyond a password to gain access, such as a fingerprint or one-time code sent to a mobile device.

In addition, organizations can monitor for attempts to reuse exposed credentials and implement automated systems to block these attempts. It is also important to educate employees about the importance of strong passwords and the risks of reusing passwords.

3. Exposed Credentials

3.7 — Restrict service account access

Typical Owner: Identity Access Management Team (IDAM)
MITRE Alignment: M1026
NIST CSF Alignment: PR.AC-4

Restricting service account access is important to prevent unauthorized access to critical systems and sensitive data. Service accounts are used to perform automated tasks, and are often granted elevated privileges to access critical systems and data. If these accounts are compromised, an attacker can gain access to sensitive data, manipulate systems, and execute malicious code.

To restrict service account access, your organization can:

- Identify all service accounts in use: Determine the purpose of each account, and identify the systems and data it has access to.
- Implement the principle of least privilege: Restrict the privileges of each service account to the minimum required for it to perform its designated function.
- Securely manage service account passwords: Ensure that service account passwords are securely stored and rotated regularly.
- Monitor and log service account activity: Regularly review service account activity logs to identify any suspicious or unauthorized access attempts.
- Implement two-factor authentication: Require two-factor authentication for service accounts to prevent unauthorized access even if the account credentials are compromised.

By taking these steps, your organization can significantly reduce the risk of service account compromise and prevent unauthorized access to critical systems and sensitive data.

3. Exposed Credentials

3.8 — Monitor for account takeover (including real time alerts on exposed credentials)

Typical Owner: SOC
MITRE Alignment: DS0028
NIST CSF Alignment: DE.CM-3

Monitoring for account takeover is an essential part of an effective cybersecurity program. Account takeover occurs when an attacker gains unauthorized access to a user's account, usually through the use of stolen credentials. Once an attacker gains access to a user's account, they can use it to steal sensitive data, compromise other accounts, or even carry out fraudulent activities on behalf of the user.

To monitor for account takeover, your organization should implement a security monitoring system that includes real-time alerts on exposed credentials. This system should be able to detect unusual activity, such as logins from unknown locations or devices, and alert security teams to potential account takeover attempts. Additionally, your organization should regularly review and analyze logs and other security data to identify potential account takeover incidents.

There are several steps your organization can take to monitor for account takeover:

- Implement multi-factor authentication (MFA): MFA requires users to provide additional information, such as a code sent to their phone, in addition to their username and password to access their account. This can significantly reduce the risk of account takeover by adding an extra layer of security.
- Use a password manager: A password manager can help users generate and securely store unique passwords for each of their accounts. This can reduce the risk of password reuse, which can lead to account takeover.
- Monitor user behavior: Your organization should establish baseline user behavior patterns and monitor for any deviations from those patterns. For example, if a user typically logs in from a certain device or location, an alert should be triggered if they suddenly log in from a new location or device.
- Regularly review access logs: Your organization should review access logs to identify any unauthorized logins or suspicious activity. This should include regular reviews of privileged account access logs, which can help detect attempts by attackers to gain elevated access to sensitive systems.
- Conduct regular security awareness training: Your organization should provide regular training to employees on best practices for password security and how to identify and report suspicious activity. This can help employees become more aware of the risks of account takeover and take proactive steps to protect their accounts.

3. Exposed Credentials

3.9 — Monitor for MFA configuration changes

Typical Owner: SOC
MITRE Alignment: M1032
NIST CSF Alignment: DE.CM-3

Monitoring for MFA (multi-factor authentication) configuration changes is important because it helps ensure that employees' accounts remain secure and protected from unauthorized access. If an attacker gains access to an employee's credentials, they may attempt to disable or modify MFA settings to make it easier to access the account in the future.

To monitor for MFA configuration changes, your organization can implement automated alerts or notifications that are triggered whenever MFA settings are modified or disabled. This can be done through a combination of logging and monitoring tools that track changes to MFA settings, as well as through periodic manual checks of employee accounts to ensure that MFA is still enabled and properly configured. In addition, regular employee education and training can help reinforce the importance of maintaining strong MFA settings and reporting any suspicious activity related to account access.

3. Exposed Credentials

3.10 — Monitor for new MFA registrations

Typical Owner: SOC
MITRE Alignment: DS0028
NIST CSF Alignment: DE.CM-3

Monitoring for new MFA registrations is important because it can indicate potential unauthorized access attempts or insider threats. If an attacker gains access to an employee's account credentials, they may attempt to register their own MFA device to bypass the existing MFA configuration and gain full access to the account.

To monitor for new MFA registrations, your organization can implement a system that tracks changes to MFA configurations and alerts security personnel when a new MFA device is registered. This system can also monitor for unusual activity such as multiple new device registrations within a short period of time and device registrations from unusual geographic locations.

Additionally, your organization can require employees to notify IT or security personnel if they register a new MFA device and implement a process to verify the legitimacy of new device registrations. This can help to prevent unauthorized access attempts and improve the overall security posture of your organization.

4. Exposed Remote Services

4.1 — Identify exposed web portals

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1133
NIST CSF Alignment: ID.AM-4

Identifying exposed web portals, such as login pages, is important for organizations because it allows them to assess potential attack surfaces and vulnerabilities that may be exploited by threat actors. By identifying these portals, organizations can better understand the scope of their attack surface and take steps to secure and monitor them.

One way to identify exposed web portals is through the use of web application scanning tools. These tools can scan an organization's web applications and identify potential vulnerabilities, including exposed login pages or other sensitive portals.

Additionally, organizations can conduct manual assessments by reviewing their own web applications or searching for them on the internet using search engines or other tools. It is important for organizations to regularly assess their web applications and portals to ensure they remain secure and to quickly identify any new potential attack surfaces.

4. Exposed Remote Services

4.2 — Identify exposed shadow IT

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1133
NIST CSF Alignment: ID.AM-4

Identifying exposed shadow IT is important because it can pose a significant security risk to an organization. Employees may use unapproved applications, software, or services that may not have proper security controls or may be vulnerable to cyberattacks. To identify shadow IT, organizations can use network monitoring tools, data loss prevention software, or conduct regular audits of employee systems and devices. It is also important to educate employees about the risks of using unapproved applications and to provide alternative solutions that meet the organization's security standards. Once identified, organizations should take steps to mitigate the risks associated with shadow IT, including blocking or restricting access to unapproved applications or services, and implementing security controls to prevent unauthorized access to sensitive information.

4. Exposed Remote Services

4.3 — Identify exposed infrastructure

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1133
NIST CSF Alignment: ID.AM-4

Identifying exposed infrastructure such as VPN, SSH, and RDP is important because it helps to reduce the risk of unauthorized access to the organization's network and systems. Attackers can use open ports and services to gain entry into the network and launch attacks, so it's essential to monitor and secure these points of entry.

4. Exposed Remote Services

4.4 — Manage shadow IT / remote access

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1030
NIST CSF Alignment: PR.AC-3

Shadow IT and remote access can pose significant security risks to an organization. It is essential to manage and control the use of shadow IT and remote access to mitigate these risks.

Here are some steps to manage shadow IT and remote access:

- Develop a shadow IT policy: Create a policy that outlines what shadow IT is, what the risks are, and what the consequences are for non-compliance.
- Identify and inventory shadow IT: Discover and catalog all the unauthorized applications, software, and services that employees use to perform their work.
- Assess the risks: Evaluate the risks associated with each shadow IT and remote access tool to determine if they are acceptable and if they meet the organization's security standards.
- Implement security controls: Implement security controls to protect the organization's network, data, and applications from unauthorized access and data exfiltration.
- Train employees: Educate employees on the risks associated with shadow IT and remote access and the importance of complying with the organization's policies and procedures.

4. Exposed Remote Services

4.5 — Implement an allowlist & limit brute force attempts

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1035
NIST CSF Alignment: PR.AC-1

Implementing an allowlist and limiting brute force attempts can help prevent unauthorized access to company resources and increase overall security.

4. Exposed Remote Services

4.6 — Establish an email gateway with best practices

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1031
NIST CSF Alignment: PR.IP-1

Establishing an email gateway with best practices such as email filters and sandboxing attachments is essential for protecting your organization from social engineering attacks for several reasons:

- Preventing malware: An email gateway with proper filters can detect and block malware-laden emails before they reach the recipient's inbox. Sandboxing can also be used to test and isolate attachments that are not clearly malicious, but could potentially harbor malware. This helps prevent the spread of malware within your organization's network and reduces the risk of data breaches and other security incidents.
- Protecting against phishing attacks: Email filters can also help detect and block phishing emails, which are designed to trick recipients into divulging sensitive information. By blocking these emails, you can reduce the risk of your employees falling victim to phishing scams and protect your organization from potential data breaches.
- Enhancing email security: An email gateway can provide additional layers of security to your email system. By implementing best practices such as email filters and sandboxing, you can ensure that your email system is protected against a wide range of threats and vulnerabilities.

To establish an email gateway with best practices, consider the following steps:

- Choose a reliable email gateway provider: Look for a provider with a track record of providing effective email security solutions and good customer support.
- Configure email filters: Configure filters to block known malware and phishing attacks, as well as suspicious attachments and emails from unknown sources.
- Implement sandboxing: Use sandboxing technology to test attachments that are not clearly malicious, but could potentially harbor malware.
- Set up monitoring and alerts: Set up monitoring and alerts to detect and respond to potential threats in real-time.
- Train employees: Educate employees on best practices for email security and how to recognize and report suspicious emails.

By establishing an email gateway with best practices, your organization can better protect itself from social engineering attacks and other email-based threats.

4. Exposed Remote Services

4.7 — Implement enterprise DNS anti-spoofing techniques

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1054
NIST CSF Alignment: PR.AC-4

Implementing enterprise DNS anti-spoofing techniques such as improving DMARC, DKIM, and SPF settings can help protect your organization from social engineering attacks in several ways:

- Email authentication: DMARC, DKIM, and SPF are email authentication protocols that verify the authenticity of incoming emails. By implementing these protocols, your organization can prevent spoofed emails from reaching your employees' inboxes. Spoofed emails can be used in social engineering attacks such as phishing and spear-phishing.
- Brand protection: Implementing these protocols can also help protect your brand reputation. Spoofed emails that appear to come from your organization can damage your reputation and erode trust with your customers.
- Compliance: Implementing these protocols may also be required for compliance with regulations such as GDPR and HIPAA, which require organizations to protect personal data.

To implement enterprise DNS anti-spoofing techniques, your organization can follow these steps:

- Identify your organization's domain names: Identify the domain names used by your organization for email communications.
- Implement SPF: Set up Sender Policy Framework (SPF) records for your domain names to specify which IP addresses are authorized to send emails on behalf of your organization.
- Implement DKIM: Set up DomainKeys Identified Mail (DKIM) for your domain names to sign outgoing emails and verify the authenticity of incoming emails.
- Implement DMARC: Set up Domain-based Message Authentication, Reporting & Conformance (DMARC) to define how your organization handles emails that fail SPF and DKIM authentication checks.
- Monitor and analyze DMARC reports: Monitor and analyze DMARC reports to identify any suspicious activity and take appropriate action.

Overall, implementing enterprise DNS anti-spoofing techniques is an important step in protecting your organization from social engineering attacks. By implementing these protocols, your organization can prevent spoofed emails from reaching your employees' inboxes, protect your brand reputation, and comply with regulations.

5. Exposed Sensitive Data

5.1 — Identify exposed sensitive data in shadow IT

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1593
NIST CSF Alignment: ID.RA-2

Your organization should identify exposed sensitive data in shadow IT to prevent data breaches and unauthorized access to sensitive information.

5. Exposed Sensitive Data

5.2 — Identify exposed sensitive data in third parties

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1593
NIST CSF Alignment: ID.RA-2

Identifying exposed sensitive data in third-party platforms such as Github is important for maintaining data privacy and security. This helps to prevent data breaches and unauthorized access to confidential information.

5. Exposed Sensitive Data

5.3 — Identify exposed confidential and risky keywords

Typical Owner: Vulnerability Management / Red Team
MITRE Alignment: T1593
NIST CSF Alignment: ID.RA-2

Your organization should identify exposed confidential and risky keywords in social media and the public web to prevent sensitive information from being disclosed publicly and to proactively identify potential risks to your organization's reputation, security, and operations.

5. Exposed Sensitive Data

5.4 — Request takedown(s) of sensitive data

Typical Owner: Privacy Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-6

Your organization should request takedown(s) of sensitive data to protect the confidentiality and privacy of individuals and sensitive information. Sensitive data may include personally identifiable information (PII), protected health information (PHI), financial information, intellectual property, and other confidential information. If this information is posted publicly or shared without authorization, it can put individuals and organizations at risk for identity theft, fraud, and other malicious activities.

To request a takedown of sensitive data, your organization can take the following steps:

- Identify the website or platform where the sensitive data is posted or shared.
- Locate the site's terms of service or user agreement to determine the process for requesting a takedown.
- Gather evidence of the sensitive data, including screenshots or links to the content.
- Follow the site's procedure for submitting a takedown request. This may include filling out a form or sending an email to the platform's designated contact.
- Provide all necessary information and evidence to support your request, including the legal basis for the takedown (if applicable).
- Monitor the platform to ensure the sensitive data has been removed, and follow up with the platform if necessary.

It's important to note that the takedown process can vary depending on the platform or website, and some may have more complex procedures or requirements. It's also a good idea to consult with legal counsel to ensure compliance with applicable laws and regulations.

5. Exposed Sensitive Data

5.5 — Monitor channels where sensitive data cannot be removed

Typical Owner: Threat Intel
MITRE Alignment: M1019
NIST CSF Alignment: DE.CM-7

Organizations should monitor channels where sensitive data cannot be removed, such as the dark web, to detect and mitigate potential threats to their sensitive information. By monitoring these channels, organizations can identify if their sensitive data has been exposed, sold, or traded on the dark web, and take necessary actions to prevent further damage.

To monitor the dark web and other channels, organizations can use a variety of tools and techniques, including:

- Dark web monitoring services: These services scan the dark web for mentions of an organization's name, sensitive data, or other relevant keywords, and alert the organization if anything is found.
- Data breach notification services: These services monitor various sources for data breaches that may affect an organization, including the dark web, and notify the organization if any of their data has been compromised.
- Web crawlers and scrapers: These tools can be used to collect data from various websites, including the dark web, and analyze it for potential threats.
- Threat intelligence platforms: These platforms gather data from various sources, including the dark web, and provide insights into potential threats and vulnerabilities.
- Human intelligence: This involves utilizing trained professionals to actively search for and monitor the dark web and other channels where sensitive data may be exposed.

To request takedown of sensitive data on the dark web or other channels, organizations can work with law enforcement agencies, dark web monitoring services, or cybersecurity firms. They can provide evidence of the exposure and request the removal of the sensitive data. However, it's important to note that complete removal of data from the dark web or other channels may not always be possible. Therefore, it's essential for organizations to take proactive measures to protect their sensitive data and prevent exposure in the first place.

5. Exposed Sensitive Data

5.6 — Flood with rogue data to generate noise

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: RS.MI-2

Flood data brokers with rogue data is a technique that can be used to generate noise and protect your organization from social engineering attacks. The idea behind this technique is to flood data brokers with fake or inaccurate information, making it difficult for attackers to identify real information about your organization.

Here are some reasons why your organization should flood data brokers with rogue data:

- Create confusion: By flooding data brokers with fake or inaccurate information, attackers will find it more difficult to differentiate between real and fake information, making it harder for them to target your organization.
- Reduce accuracy: By providing inaccurate information, data brokers will have a more difficult time accurately profiling your organization, which can reduce the accuracy of any data that attackers may use to target your organization.
- Increase cost: By flooding data brokers with rogue data, your organization can increase the cost for attackers to gather accurate information about your organization, making it less cost-effective for them to conduct social engineering attacks.

Here are some steps your organization can take to flood data brokers with rogue data:

- Identify data brokers: Identify the data brokers that may have information about your organization.
- Create fake profiles: Create fake profiles or personas with fake information, including fake names, addresses, and other personal information.
- Populate the data: Populate the data brokers with fake or inaccurate information by submitting the fake profiles to the data brokers.
- Monitor for leaks: Monitor for any leaks of the fake or inaccurate information to ensure that the data brokers are not inadvertently distributing this information to attackers.
- Regularly update data: Regularly update the fake profiles with new fake or inaccurate information to maintain a high level of noise and confusion.

It is important to note that this technique may not be effective against all types of social engineering attacks and may require a significant amount of resources to implement. Additionally, flooding data brokers with rogue data may be illegal or violate the terms of service of some data brokers, so it is important to consult with legal counsel before implementing this technique.

6. Third Party Risk Management

6.1 — Identify third parties that have direct network access and access to systems

Typical Owner: GRC (Governance Risk and Compliance) Team
MITRE Alignment: M1047
NIST CSF Alignment: ID.SC-2

Preventing social engineering attacks is crucial for safeguarding your organization's sensitive information. Identifying third parties with direct network access and system privileges is an important step in mitigating potential risks. Here's why you should do it and how to go about it:

- Assess Vulnerabilities: Third parties may inadvertently become a target for social engineering attacks, allowing unauthorized access to your systems. Identifying these parties helps you understand potential vulnerabilities and proactively address them.
- Protect Data: By knowing which third parties have access to your network and systems, you can implement appropriate security measures to safeguard your data from unauthorized access, data breaches, or misuse.
- Compliance and Regulations: Many industries have specific compliance requirements that mandate monitoring and managing third-party access. Identifying these parties helps ensure compliance and protects your organization from legal and regulatory issues.

To identify third parties with direct network access and system privileges, follow these steps:

- Create an Inventory: Compile a comprehensive list of all third parties that have access to your network or systems. This may include vendors, contractors, service providers, and partners.
- Evaluate Access Levels: Determine the level of access each third party has to your network and systems. Identify whether they have administrative privileges, direct network access, or any special authorizations.
- Assess Security Practices: Review the security protocols and practices of each third party. Ensure they follow robust security measures, such as strong authentication, encryption, regular vulnerability assessments, and employee training on social engineering awareness.
- Implement Risk Mitigation Measures: Based on the assessment, implement appropriate measures to mitigate potential risks. This may include limiting access privileges, implementing multi-factor authentication, conducting regular audits, and enforcing security policies and contracts.
- Ongoing Monitoring: Regularly review and update the list of third parties with network access and system privileges. Continuously monitor their activities and periodically reassess their security practices to maintain a proactive security posture.

Remember, preventing social engineering attacks requires a holistic approach that includes employee education, strong technical controls, and continuous monitoring. By identifying and managing third parties with network access and system privileges, you can significantly reduce the risk of social engineering attacks on your organization.

6. Third Party Risk Management

6.2 — Monitor third parties that have direct network access and access to systems

Typical Owner: SOC
MITRE Alignment: M1018
NIST CSF Alignment: DE.CM-6

Monitoring third parties with direct network access and system privileges is crucial for preventing social engineering attacks and safeguarding your organization's security. Here's why you should do it and how to go about it:

Why monitor third parties with network access:

- Risk Mitigation: Monitoring helps identify any suspicious or unauthorized activities performed by third parties. It enables early detection of potential security breaches and allows prompt action to mitigate risks.
- Compliance and Regulations: Many industries have compliance requirements that necessitate monitoring third-party access. By actively monitoring these parties, you ensure adherence to regulations and protect your organization from legal and regulatory consequences.
- Incident Response: Timely monitoring enables swift incident response in case of any security breaches or suspicious activities. It allows you to investigate and take necessary measures to minimize the impact on your systems and data.

How to monitor third parties with network access:

- Access Logs and Auditing: Implement comprehensive logging and auditing mechanisms to capture all activities performed by third parties. This includes tracking logins, system access, file transfers, and any changes made to configurations or data.
- User Behavior Analytics (UBA): Utilize UBA tools to analyze the behavior patterns of third parties accessing your network and systems. These tools can detect anomalies and deviations from normal behavior, triggering alerts for further investigation.
- Regular Audits and Reviews: Conduct periodic audits of third-party activities to ensure compliance with security policies and contractual obligations. Review their access privileges, authentication mechanisms, and adherence to security best practices.
- Incident Response Planning: Develop a robust incident response plan that outlines the steps to be taken in case of security incidents involving third parties. Include protocols for notifying relevant stakeholders, conducting investigations, and implementing necessary remediation measures.
- Communication and Collaboration: Maintain open lines of communication with third parties to address any security concerns, clarify expectations, and reinforce security awareness. Collaboration and information sharing can help proactively identify potential risks and enhance security measures.
- Security Assessments: Regularly assess the security posture of third parties through questionnaires, security audits, or penetration testing. This helps evaluate their security practices and identify areas for improvement.
- Contractual Obligations: Ensure that contracts and agreements with third parties clearly define security requirements, responsibilities, and the scope of monitoring. Include provisions for periodic security reviews and reporting on their compliance.

Remember, monitoring third parties with network access is an ongoing process. Continuously evaluate and refine your monitoring strategies to adapt to evolving threats and technologies. By actively monitoring these parties, you enhance your organization's security posture and reduce the risks associated with social engineering attacks.

6. Third Party Risk Management

6.3 — Establish authenticated communications channel with third parties to reduce spoofing

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1030
NIST CSF Alignment: PR.PT-4

Establishing an authenticated communications channel with third parties can help reduce the risk of spoofing attacks, where an attacker impersonates a trusted third party to gain access to sensitive information or conduct fraudulent activities. By verifying the identity of the third party and ensuring that communications are secure and confidential, organizations can reduce the risk of data breaches and other security incidents.

To establish an authenticated communications channel with third parties, organizations can follow these steps:

- Identify the third parties with whom you need to establish secure communications. This may include vendors, partners, customers, and other external entities.
- Determine the appropriate level of security for the communications channel. This may depend on the sensitivity of the information being shared and the risk associated with a potential breach.
- Choose a secure communications protocol such as encrypted messaging apps, authenticated video conferencing software, and authenticated email services that leverage DKIM, SPF, and DMARC.
- Establish a set of authentication credentials, such as usernames and passwords or digital certificates, that are unique to each third party and are used to verify their identity when connecting to the communications channel.
- Train employees and third-party users on how to use the authenticated communications channel and ensure that they understand the importance of maintaining its security.
- Regularly monitor the communications channel for suspicious activity and conduct security assessments to ensure that it remains secure over time.

6. Third Party Risk Management

6.4 — Build and establish third party and supply chain policies, processes, and procedures

Typical Owner: GRC (Governance Risk and Compliance) Team
MITRE Alignment: N/A
NIST CSF Alignment: PR.AT-3

Your organization should build and establish third party and supply chain policies, processes, and procedures to ensure that the security and privacy of your sensitive data are adequately protected, even when it is being shared with or accessed by third-party vendors or partners. Third-party and supply chain risks can be a significant threat to your organization's security and data protection, as many breaches and attacks have been initiated through a vulnerable third party.

To build and establish third party and supply chain policies, processes, and procedures, you can follow these steps:

- Identify and classify third parties and supply chain partners based on their level of access to your sensitive data and the risk level associated with their activities.
- Define and document the minimum security and privacy requirements that third parties and supply chain partners must adhere to, such as access controls, data encryption, incident response, and compliance with relevant regulations.
- Establish a clear process for vetting and selecting third parties and supply chain partners, including due diligence and ongoing monitoring.
- Implement contractual language that defines the expectations and responsibilities of both parties in terms of data security and privacy.
- Train your employees and third-party partners on the importance of data security and privacy, as well as your policies and procedures.
- Regularly review and assess the effectiveness of your policies, processes, and procedures to ensure they are up-to-date and effective.

6. Third Party Risk Management

6.5 — Require service providers to securely manage your data

Typical Owner: GRC (Governance Risk and Compliance) Team
MITRE Alignment: N/A
NIST CSF Alignment: PR.AT-3

Your organization should require service providers to securely manage your data to ensure that your sensitive information is protected and not compromised by the service provider's security vulnerabilities or negligence. By doing so, your organization can maintain control and ownership over your data and ensure that it is being handled in a manner that is compliant with industry standards and regulations.

To require service providers to securely manage your data, you can take the following steps:

- Conduct due diligence on potential service providers: Before engaging a service provider, conduct a thorough background check to ensure that they have a good reputation and a history of secure data management.
- Include security requirements in contracts: Ensure that your contracts with service providers include specific security requirements, such as data encryption, access controls, incident response procedures, and leveraging the HASP Framework.
- Conduct regular security audits: Regularly audit your service providers for human OSINT vulnerabilities to ensure that they are meeting the agreed-upon security requirements and that their security controls are up to date.
- Establish incident response protocols: Establish protocols for incident response in the event of a data breach or other security incident involving a service provider.
- Monitor third-party security risks: Continuously monitor for third-party security risks and take appropriate action to mitigate those risks.
- Provide training and awareness: Provide training and awareness to your employees and service providers on the importance of secure data management and the risks associated with inadequate security practices.

By taking these steps, your organization can reduce the risk of data breaches and ensure that your sensitive information is being securely managed by service providers.

7. Indicators of Attack

7.1 — Monitor for suspicious external accounts

Typical Owner: SOC
MITRE Alignment: T1585.001
NIST CSF Alignment: DE.CM-7

Your organization should monitor for suspicious external accounts to protect against social engineering attacks and prevent unauthorized access to sensitive information. Cyber criminals can create fake accounts on social media platforms like LinkedIn to impersonate legitimate users and gain access to confidential data.

To monitor for suspicious external accounts, your organization can:

- Set up alerts: Configure alerts to notify security personnel whenever new accounts are created with the same or similar names as key personnel in your organization.
- Regularly review accounts: Conduct regular reviews of accounts associated with your organization on social media platforms to ensure that all accounts are legitimate.
- Check for inconsistencies: Look for inconsistencies in account information, such as incomplete profiles, lack of connections, or suspicious job titles.
- Train employees: Provide regular training to employees on how to identify and report suspicious activity on social media.
- Use automated tools: Employ automated tools to monitor social media platforms and identify suspicious activity, such as unusual login locations or unusual activity on the account.

Overall, it is important to be vigilant and regularly monitor social media platforms to protect against social engineering attacks and unauthorized access to sensitive information.

7. Indicators of Attack

7.2 — Request takedowns for suspicious external accounts

Typical Owner: Privacy Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-7

If your organization identifies suspicious external accounts (e.g., LinkedIn impersonations) that are attempting to impersonate your company or its employees, it is important to take action to have them removed. Requesting takedowns can help prevent these accounts from being used for malicious purposes such as phishing or spreading misinformation.

Here are some steps your organization can take to request takedowns for suspicious external accounts:

- Gather information: Collect information about the suspicious account, including the account name, URL, and any evidence that it is impersonating your company or employees. This information can be used to report the account to the platform on which it is hosted.
- Report to the platform: Most social media and other online platforms have a process for reporting fraudulent or suspicious accounts. Look for a “Report” button or similar option on the account page and follow the instructions to report the account.
- Contact the hosting provider: If the account is hosted on a website or domain, you can contact the hosting provider and request that the account be taken down. Look up the contact information for the hosting provider and provide the evidence you have collected to support your request.
- Monitor for additional activity: After requesting a takedown, it is important to continue monitoring for additional suspicious activity. If you notice similar accounts or activity in the future, take action quickly to prevent harm.

It is also important to have a plan in place for responding to suspicious external accounts and to educate employees on how to recognize and report them.

7. Indicators of Attack

7.3 — Alert your organization about suspicious external accounts

Typical Owner: SOC
MITRE Alignment: DS0021
NIST CSF Alignment: RS.MI-3

Your organization should alert its employees about suspicious external accounts in order to raise awareness and prevent potential threats such as phishing and social engineering attacks. By being vigilant and reporting suspicious activity, employees can help prevent unauthorized access to sensitive information, financial loss, and reputational damage.

To alert your organization about suspicious external accounts, you can establish a reporting mechanism such as a dedicated email address or a hotline where employees can report any suspicious activity. You can also provide training and education to employees on how to identify suspicious activity, such as phishing emails, fake social media profiles, and other forms of social engineering. Additionally, you can implement security measures such as multi-factor authentication, strong passwords, and regular security audits to protect against external threats.

To ensure that reports of suspicious activity are properly investigated and addressed, you can establish a security incident response team that is responsible for monitoring and responding to security incidents. This team should have a clear set of procedures and protocols in place for investigating suspicious activity, notifying relevant parties, and taking appropriate action to mitigate the risk.

It is also important to work with law enforcement and other relevant authorities to report suspicious activity and cooperate with any investigations that may be necessary. By taking a proactive approach to identifying and addressing suspicious external accounts, your organization can better protect itself from potential security threats.

7. Indicators of Attack

7.4 — Monitor for suspicious domains

Typical Owner: SOC
MITRE Alignment: T1583.001
NIST CSF Alignment: DE.CM-7

Your organization should monitor for suspicious domains to identify and prevent potential phishing attacks, malware infections, and other cyber threats that may originate from fake or malicious domains. Suspicious domains may include typosquatting domains, lookalike domains, and other domains that may be used to deceive users and trick them into revealing sensitive information or downloading malware.

7. Indicators of Attack

7.5 — Block suspicious domains

Typical Owner: Network & Infrastructure Team
MITRE Alignment: DS0038
NIST CSF Alignment: PR.AC-4

Blocking suspicious domains is an important measure to protect your organization from social engineering attacks. Here are some reasons why:

- Prevents malicious activities: Suspicious domains can be used for a variety of malicious activities, such as phishing, malware distribution, and command and control (C&C) communication. Blocking these domains can prevent these activities from occurring.
- Reduces risk of data loss: Social engineering attacks often aim to steal sensitive information, such as login credentials or financial data. Blocking suspicious domains can help prevent this information from being transmitted to attackers.
- Enhances security posture: Blocking suspicious domains can enhance the overall security posture of your organization by reducing the risk of successful social engineering attacks.

To block suspicious domains, your organization can follow these steps:

- Identify suspicious domains: Identify the domains that are suspicious and should be blocked.
- Implement domain blocking solution: Implement a domain blocking solution that allows your organization to block access to suspicious domains.
- Monitor and update blocked domains: Regularly monitor and update the list of blocked domains to ensure that new suspicious domains are added and obsolete domains are removed.
- Train employees: Train employees on how to recognize and respond to social engineering attacks related to suspicious domains.

Overall, blocking suspicious domains is an important measure to protect your organization from social engineering attacks. By identifying suspicious domains, implementing a domain blocking solution, monitoring and updating the list of blocked domains, and training employees, your organization can better protect against social engineering attacks related to suspicious domains.

7. Indicators of Attack

7.6 — Monitor for certificate/token stealing

Typical Owner: SOC
MITRE Alignment: M1018
NIST CSF Alignment: DE.CM-1

Monitoring for certificate/token stealing is an important aspect of protecting your organization from social engineering attacks. Here are some reasons why:

- Protects sensitive information: Certificates and tokens are often used to access sensitive information or systems. Monitoring for certificate/token stealing can help prevent unauthorized access to this information.
- Reduces risk of identity theft: If a certificate or token is stolen, it can be used to impersonate a legitimate user or system. This can lead to identity theft and other security issues.
- Enhances security: Monitoring for certificate/token stealing can help enhance the overall security posture of your organization by reducing the risk of successful social engineering attacks.

To monitor for certificate/token stealing, your organization can follow these steps:

- Identify certificates and tokens: Identify the certificates and tokens used by your organization to access sensitive information or systems.
- Implement certificate/token monitoring solution: Implement a certificate/token monitoring solution that allows your organization to detect when certificates or tokens are stolen or used in unauthorized ways.
- Analyze monitoring data: Regularly analyze the monitoring data to detect suspicious activity related to certificate/token stealing.
- Take action: Take action when suspicious activity is detected. This can include revoking or replacing stolen certificates or tokens, and investigating potential social engineering attacks.
- Train employees: Train employees on how to recognize and respond to social engineering attacks related to certificate/token stealing.

Overall, monitoring for certificate/token stealing can help protect your organization from social engineering attacks. By identifying certificates and tokens, implementing a certificate/token monitoring solution, analyzing monitoring data, taking action, and training employees, your organization can better protect against social engineering attacks related to certificate/token stealing.

7. Indicators of Attack

7.7 — Block list of scam-likely phone numbers

Typical Owner: Network & Infrastructure Team
MITRE Alignment: M1056
NIST CSF Alignment: PR.IP-1

Blocking a list of scam-likely phone numbers can help protect your organization from social engineering attacks that use phone calls as a means of gaining access to sensitive information. Here are some reasons why:

- Reduces exposure: By blocking known scam-likely phone numbers, your organization can reduce its exposure to potential social engineering attacks via phone calls.
- Saves time: Blocking known scam-likely phone numbers can save time for employees who may be targeted by these attacks, as they will not have to spend time responding to or investigating suspicious phone calls.
- Enhances security: Blocking known scam-likely phone numbers can help enhance the overall security posture of your organization by reducing the risk of successful social engineering attacks.

To block a list of scam-likely phone numbers, your organization can follow these steps:

- Identify a list of known scam-likely phone numbers: Research and identify a list of phone numbers that are known to be associated with social engineering attacks.
- Implement a phone number blocking solution: Implement a phone number blocking solution that allows your organization to block calls from specific phone numbers.
- Update the list of blocked numbers: Regularly update the list of blocked phone numbers as new threats emerge.
- Train employees: Train employees on how to recognize and respond to social engineering attacks via phone calls. This can include providing guidance on what to do if they receive a suspicious phone call on either their work or personal devices.
- Monitor for new threats: Monitor for new threats and adjust the list of blocked phone numbers accordingly.

Overall, blocking a list of known scam-likely phone numbers can help protect your organization from social engineering attacks via phone calls. By identifying a list of known threats, implementing a phone number blocking solution, updating the list of blocked numbers, training employees, and monitoring for new threats, your organization can better protect against social engineering attacks.

8. Lack of Social Engineering Understanding and Protection

8.1 — Train employees on social engineering attacks

Typical Owner: Security Awareness Team
MITRE Alignment: M1017
NIST CSF Alignment: PR.AT-1

Training employees on social engineering attacks is essential to protect your organization from social engineering threats. Here are some reasons why:

- Increased awareness: By training employees on social engineering attacks, they will be better equipped to recognize potential threats and respond appropriately. This can increase their awareness and reduce the likelihood of falling victim to an attack.
- Improved response: If a social engineering attack does occur, trained employees will be better prepared to respond, minimizing the impact of the attack on the organization.
- Better security posture: Training employees on social engineering attacks can help improve the organization's overall security posture by identifying potential vulnerabilities and reinforcing security policies and procedures.

To train employees on social engineering attacks, your organization can follow these steps:

- Develop a training plan: Develop a plan for training employees on social engineering attacks. This should include the types of attacks to be covered, the frequency of training, and the metrics to be tracked.
- Select training tools: Select training tools that are appropriate for your organization's needs.
- Conduct training sessions: Conduct training sessions for employees, using the selected training tools to simulate social engineering attacks. This should include providing guidance on how to recognize and respond to potential attacks, whether they occur at work or at home.
- Analyze results: Analyze the results of the training exercises to identify areas of weakness and potential vulnerabilities. Use this information to refine your organization's security measures and improve employee training.
- Provide feedback: Provide feedback to employees who participate in the training exercises. This should include information on how they performed and guidance on how they can improve their responses to potential attacks.

Overall, training employees on social engineering attacks is critical to protecting your organization from social engineering threats. By developing a training plan, selecting training tools, conducting training sessions, analyzing results, and providing feedback, your organization can improve its security posture and better protect against potential attacks.

8. Lack of Social Engineering Understanding and Protection

8.2 — Provide employees social engineering phishing simulation training

Typical Owner: Security Awareness Team
MITRE Alignment: M1017
NIST CSF Alignment: PR.AT-1

Providing employees with social engineering phishing simulation training is essential for protecting your organization from social engineering attacks. Here are some reasons why:

- Increased awareness: Social engineering phishing simulation training can help employees understand how social engineering attacks work and how to identify and respond to them. This can improve their awareness and reduce the likelihood of falling victim to an attack.
- Proactive defense: By simulating social engineering attacks, employees can gain hands-on experience in identifying and responding to such attacks. This can help build a proactive defense against social engineering attacks, enabling employees to be more vigilant and better prepared to protect against potential attacks.
- Continuous improvement: Social engineering phishing simulation training can help your organization identify areas of weakness in its security posture. By analyzing employee responses to simulated attacks, your organization can identify areas for improvement and continually refine its security measures.

To implement social engineering phishing simulation training, your organization can follow these steps:

- Develop a training plan: Develop a plan for social engineering phishing simulation training. This should include the frequency of training, the types of simulations to be used that represent actual risks, and the metrics to be tracked.
- Select simulation tools: Select simulation tools that are appropriate for your organization's needs.
- Conduct training sessions: Conduct training sessions for employees, using the selected simulation tools to simulate social engineering attacks. This should include providing guidance on how to identify and respond to potential attacks.
- Analyze results: Analyze the results of the simulation exercises to identify areas of weakness and potential vulnerabilities. Use this information to refine your organization's security measures and improve employee training.
- Provide feedback: Provide feedback to employees who participate in the simulation exercises. This should include information on how they performed and guidance on how they can improve their responses to potential attacks.

Overall, providing social engineering phishing simulation training to employees is an effective way to protect your organization from social engineering attacks. By developing a training plan, selecting simulation tools, conducting training sessions, analyzing results, and providing feedback, your organization can improve its security posture and better protect against potential attacks.

8. Lack of Social Engineering Understanding and Protection

8.3 — Train security team on social engineering tactics

Typical Owner: Security Awareness Team
MITRE Alignment: M1017
NIST CSF Alignment: PR.AT-5

Training the security team on social engineering tactics is crucial to protect your organization from social engineering attacks. Here are some reasons why:

- Early detection: The security team is responsible for detecting and responding to potential security threats, including social engineering attacks. By training the security team on social engineering tactics, they will be better equipped to identify potential attacks and respond to them promptly.
- Improved incident response: If a social engineering attack does occur, the security team will be responsible for responding to the incident. By providing training on social engineering tactics, the security team will be better prepared to handle such incidents, minimizing the potential impact on the organization.
- Continuous improvement: Training the security team on social engineering tactics can help your organization stay up-to-date on the latest tactics and trends in social engineering attacks. This can enable your organization to continually improve its security posture and protect against future attacks.

To train the security team on social engineering tactics, your organization can follow these steps:

- Develop a training plan focused on actual threats: Develop a training plan that covers the basics of social engineering, common tactics used in social engineering attacks, and how to identify and respond to potential attacks.
- Provide training materials: Provide training materials, such as videos, articles, and case studies, to the security team. These materials should cover the latest trends and tactics in social engineering attacks.
- Conduct targeted training sessions: Conduct training sessions for the security team, either in-person or online. These sessions should provide an opportunity for the security team to ask questions and discuss specific scenarios that match actual threats to identified human vulnerabilities.
- Test knowledge: Test the knowledge of the security team by conducting simulated social engineering attacks. This can help identify any knowledge gaps and provide an opportunity to improve the security team's response to potential attacks.
- Provide ongoing training: Provide ongoing training to the security team to ensure that they are up-to-date on the latest trends and tactics in social engineering attacks.

Overall, training the security team on social engineering tactics is critical to protecting your organization from social engineering attacks. By developing a training plan, providing training materials, conducting training sessions, testing knowledge, and providing ongoing training, your organization can improve its security posture and better protect against potential attacks.

8. Lack of Social Engineering Understanding and Protection

8.4 — Build and establish social engineering policies, processes, and procedures

Typical Owner: Security Awareness Team
MITRE Alignment: N/A
NIST CSF Alignment: PR.IP-1

Social engineering attacks are a type of cyber attack that target human behavior rather than technology. They exploit psychological weaknesses to trick individuals into divulging sensitive information, taking malicious actions, or downloading malware.

It is important for organizations to keep up to date on recent social engineering attacks and methods to protect against them because these attacks can have severe consequences. Social engineering attacks can result in data breaches, financial losses, reputational damage, and even legal liability. Additionally, social engineering attacks are becoming increasingly sophisticated and difficult to detect, so it is crucial for organizations to stay informed and prepared.

To keep up to date on social engineering attacks, organizations should implement the following strategies:

- Regular employee training: Organizations should provide regular training to employees on social engineering attacks and how to identify and avoid them. Training should include real-world examples and simulations of social engineering attacks to help employees recognize and respond appropriately.
- Conduct security assessments: Organizations should conduct regular security assessments to identify vulnerabilities and weaknesses that could be exploited in a social engineering attack. This can include phishing simulations, penetration testing, and vulnerability scans.
- Stay informed: Organizations should stay up to date on the latest social engineering tactics and trends by following industry news and subscribing to relevant newsletters and blogs.
- Implement security policies and procedures: Organizations should implement policies and procedures that address social engineering attacks, including password management, access control, and incident response.
- Use technology to prevent and detect social engineering attacks: Organizations should use technology solutions, such as anti-phishing software and email filters, to prevent social engineering attacks. They should also monitor network traffic and behavior to detect suspicious activity.

By implementing these strategies, organizations can help protect themselves from social engineering attacks and mitigate the risk of a successful attack.

8. Lack of Social Engineering Understanding and Protection

8.5 — Give employees a way to report phishing/smshing

Typical Owner: Security Awareness Team
MITRE Alignment: N/A
NIST CSF Alignment: PR.IP-1

Giving employees a way to report phishing/smishing is essential for protecting your organization from social engineering attacks. Here are some reasons why:

- Early detection: Promptly identifying phishing/smishing attacks is critical to minimizing their impact. Employees who have a way to report such attacks can help your organization detect and respond to them early, reducing the risk of data breaches or loss of sensitive information.
- Employee engagement: Providing employees with a way to report phishing/smishing demonstrates that your organization values their role in cybersecurity. This can improve employee engagement and create a culture of security awareness, where employees are more likely to be vigilant against potential attacks.
- Continuous improvement: Collecting reports on phishing/smishing attacks can help your organization identify patterns and trends in attacks, enabling you to improve your security posture and better protect against future attacks.

To implement a system for reporting phishing/smishing attacks, your organization can follow these steps:

- Develop a reporting process: Create a clear and concise process for employees to report phishing/smishing attacks. This could involve a dedicated email address or web form for reporting such incidents.
- Communicate the reporting process: Communicate the reporting process to employees through training sessions, company-wide emails, or other channels. Ensure that employees understand the importance of reporting potential attacks promptly.
- Analyze reports: Analyze reports of phishing/smishing attacks to identify patterns and trends in attacks. Use this information to improve your security posture and develop targeted awareness training for employees.
- Provide feedback: Provide feedback to employees who report potential attacks. Let them know that their reports are valued and that their actions are helping to protect the organization.

Overall, giving employees a way to report phishing/smishing attacks is an important step in protecting your organization from social engineering attacks. By providing a clear reporting process, communicating the importance of reporting, analyzing reports, and providing feedback, your organization can create a culture of security awareness and improve its ability to detect and respond to potential attacks.

8. Lack of Social Engineering Understanding and Protection

8.6 — Provide near real-time responses to phishing/spoofing inquiries

Typical Owner: SOC
MITRE Alignment: DS0029
NIST CSF Alignment: PR.IP-1

Providing near real-time responses to phishing/spoofing inquiries is important for protecting your organization from social engineering attacks for several reasons:

- Reducing response time: Social engineering attacks are often time-sensitive, and attackers may try to capitalize on the window of opportunity before their attacks are detected. By providing near real-time responses to phishing/spoofing inquiries, your organization can quickly investigate and respond to potential attacks, reducing the time window for attackers to exploit vulnerabilities.
- Minimizing damage: A fast response to phishing/spoofing inquiries can help minimize the damage caused by successful attacks. For example, if an employee falls for a phishing email and inadvertently shares sensitive information, a prompt response can help limit the amount of data that is compromised.
- Maintaining customer trust: If a customer reports a phishing or spoofing attempt, they expect a quick and appropriate response. By providing near real-time responses to such inquiries, you can demonstrate your commitment to protecting customer data and maintain their trust in your organization.

To provide near real-time responses to phishing/spoofing inquiries, your organization can implement the following steps:

- Develop an incident response plan: Your organization should have a documented incident response plan that outlines the steps to take in the event of a phishing or spoofing attack. This plan should include details on who to notify, how to investigate the incident, and how to respond to affected parties.
- Establish a reporting system: Implement a system for employees and customers to report phishing and spoofing attempts. This system should be easy to use and provide clear instructions on how to report incidents.
- Assign incident response team members: Identify and train incident response team members who are responsible for investigating and responding to phishing and spoofing incidents.
- Investigate reported incidents promptly: Investigate reported incidents promptly to determine the severity of the attack and take appropriate measures to mitigate the damage.
- Communicate with affected parties: Communicate with affected parties, including customers, employees, and other stakeholders, to inform them of the incident, the steps your organization is taking to mitigate the damage, and how they can protect themselves.

By implementing these steps, your organization can provide near real-time responses to phishing/spoofing inquiries and help protect against social engineering attacks.

8. Lack of Social Engineering Understanding and Protection

8.7 — Keep up to date on recent social engineering attacks and methods

Typical Owner: Threat Intel
MITRE Alignment: M1019
NIST CSF Alignment: PR.AT-5

It is important for your organization to keep up to date on recent social engineering attacks and methods to protect from social engineering because social engineering attacks are becoming increasingly sophisticated and prevalent in today's digital landscape. Social engineering attacks can result in financial loss, data breaches, reputation damage, and legal repercussions for organizations that fall victim to them.

By staying informed about the latest social engineering tactics and vulnerabilities, your organization can implement effective security measures to mitigate the risk of such attacks. This includes educating employees about social engineering attacks, implementing security policies and procedures, and using technology solutions to monitor and prevent such attacks.

To stay up to date on recent social engineering attacks and methods to protect from social engineering, your organization can:

- Subscribe to cybersecurity news and alerts - this will ensure that your organization is aware of the latest threats and vulnerabilities.
- Conduct regular security awareness training - this will educate employees on how to recognize and respond to social engineering attacks.
- Conduct penetration testing and vulnerability assessments - this will identify potential vulnerabilities and provide recommendations for improving security measures.
- Implement security policies and procedures - this will establish guidelines and protocols for how to handle sensitive information and prevent social engineering attacks.
- Use technology solutions - this includes anti-phishing software, email filters, and other security tools that can help detect and prevent social engineering attacks.

By implementing these measures, your organization can stay up to date on recent social engineering attacks and methods to protect from social engineering, thereby reducing the risk of becoming a victim of these types of attacks.

9. Incident Response

9.1 — Identify potential attackers or threat actors involved in the incident using OSINT methods

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: ID-RA-2

Use various OSINT techniques, such as social media monitoring, search engine queries, and domain or IP address lookups, to identify potential attackers or threat actors. Correlate data with threat intelligence: Compare the data collected with known threat intelligence sources to identify any matching patterns or indicators of compromise (IOCs).

9. Incident Response

9.2 — Conduct research on the tactics, techniques, and procedures (TTPs) used by the attackers or threat actors to help prevent future incidents

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: ID-RA-2

Review all available information: Collect all available information about the incident, including logs, network traffic, and any other relevant data. Use the collected information to analyze the attack and identify the TTPs used by the attackers. Conduct open-source intelligence (OSINT) research to identify any known TTPs used by the attackers or similar groups in the past.

9. Incident Response

9.3 — Assess the incident

Typical Owner: SOC
MITRE Alignment: N/A
NIST CSF Alignment: ID-RA-2

Detect and identify the social engineering related to the incident as early as possible and determine the potential impact on the organization and its stakeholders. This can be through employee reports, system alerts, or other monitoring mechanisms.

9. Incident Response

9.4 — Isolate the incident

Typical Owner: Network & Infrastructure Team
MITRE Alignment: N/A
NIST CSF Alignment: RS.MI-1

Isolate the affected systems or accounts to prevent further compromise. This may involve disconnecting compromised devices from the network or suspending compromised user accounts.

9. Incident Response

9.5 — Preserve evidence

Typical Owner: Network & Infrastructure Team
MITRE Alignment: N/A
NIST CSF Alignment: RC.RP-1

Preserve any relevant evidence related to the incident. This includes capturing email headers, logging network activity, or taking screenshots of suspicious messages. This evidence can be essential for investigations, legal actions, or future preventive measures.

9. Incident Response

9.6 — Contain the incident

Typical Owner: SOC
MITRE Alignment: N/A
NIST CSF Alignment: RS.MI-1

Contain the incident by implementing measures to prevent further unauthorized access or data loss. Change passwords, revoke compromised access privileges, or apply security patches to vulnerable systems.

9. Incident Response

9.7 — Investigate the incident

Typical Owner: SOC
MITRE Alignment: N/A
NIST CSF Alignment: DE.AE-2

Conduct a thorough investigation to determine the scope of the incident, how it occurred, and the potential impact. Identify the methods and information used by the attacker and any vulnerabilities exploited. Collaborate with IT, security teams, and potentially law enforcement or forensic experts if necessary.

9. Incident Response

9.8 — Communicate and notify

Typical Owner: SOC
MITRE Alignment: N/A
NIST CSF Alignment: RS.CO-4

Notify the appropriate stakeholders about the incident. This includes senior management, legal counsel, and any other relevant parties. Develop a communication plan to inform employees, customers, and partners about the incident, while ensuring transparency and minimizing panic.

9. Incident Response

9.9 — Educate users and create awareness of former incident

Typical Owner: Security Awareness Team
MITRE Alignment: N/A
NIST CSF Alignment: PR.AT-1

Provide guidance and training to employees about the incident to prevent future occurrences. Reinforce security awareness, educate them about common social engineering tactics, and emphasize the importance of reporting suspicious activities.

9. Incident Response

9.10 — Update incident response plans

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: RC.IM-2

Evaluate the incident response plan based on lessons learned from the incident. Identify areas for improvement, update policies and procedures, and enhance preventive measures and tools to mitigate the risk of future social engineering attacks.

9. Incident Response

9.11 — Continuously monitor and remediate

Typical Owner: SOC
MITRE Alignment: N/A
NIST CSF Alignment: DE.CM-1

Implement ongoing monitoring and analysis to detect any residual traces of the incident and ensure that the organization's systems and data remain secure. Regularly assess and update security controls, conduct vulnerability assessments, and patch any identified weaknesses.

9. Incident Response

9.12 — Conduct and document a post-incident review

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: RC.IM-1

Conduct a post-incident review to assess the effectiveness of the response and identify areas for improvement. Document the incident, response actions, lessons learned, and recommendations for future incidents.

9. Incident Response

9.13 — Implement proactive preventive measures

Typical Owner: Threat Intel
MITRE Alignment: N/A
NIST CSF Alignment: PR.IP-7

Use tools to continuously monitor for potential threats and vulnerabilities that could lead to future incidents. Implement ongoing monitoring and analysis to detect any residual traces of the incident and ensure that the organization's systems and data remain secure. Regularly assess and update security controls, conduct vulnerability assessments, and patch any identified weaknesses.