

Checklist:

Insider Threat Prevention and Response

bch

BRADY, CHAPMAN,
HOLLAND &
ASSOCIATES

An insider threat refers to an individual who has been entrusted with access to or knowledge of an organization's operational components, personnel, physical assets, networks, systems or technology. Insider threats may stem from negligent employees, malicious insiders or third-party collaborators (e.g., vendors and suppliers). Due to their understanding of and privileges to such sensitive information and resources, insider threats have the potential to compromise organizations' most valuable assets and leave them increasingly vulnerable to various cyberattacks.

Insider threats pose significant cybersecurity risks for businesses of all sizes and sectors, often resulting in serious consequences. Specifically, cyber incidents stemming from insider threats (also known as insider events) can lead to prolonged operational disruptions, widespread data exposure, severe reputational damage and large-scale financial losses. With this in mind, it's vital for organizations to take steps to minimize insider threats. This checklist outlines key insider threat prevention and response techniques for companies to consider.

ASSESSING RISKS AND INDICATORS	YES	NO	COMMENTS
Has the organization conducted a documented risk assessment to understand its unique insider threat exposures?	☐	☐	
Has the organization identified critical company assets that could be targeted by insider threats and outlined the potential ramifications that may result from these assets being compromised?	☐	☐	
Does the organization reassess its insider threat exposures as needed (e.g., upon acquiring new assets, hiring new third-party collaborators, altering operations or implementing new workplace technology)?	☐	☐	
Is the organization aware of certain indicators (i.e., background personal, behavioral, technical and environmental) that may allude to the presence of an insider threat?	☐	☐	

PROMOTING A SECURITY CULTURE	YES	NO	COMMENTS
Has the organization fostered a positive, supportive and transparent company culture that encourages employees to take cybersecurity seriously and come forward if they notice any indicators of insider threats?	☐	☐	
Does the organization have hiring processes in place that help vet job candidates for possible insider threat exposures (e.g., interviews, character assessments, professional references and background checks)?	☐	☐	
Does the organization provide employees with routine cybersecurity training to bolster their awareness of insider threats and proper mitigation measures?	☐	☐	
Does the organization offer engaging educational programs related to insider threats and inspire employees to take ownership of their cybersecurity responsibilities?	☐	☐	
Has the organization involved company leaders and executives in insider threat mitigation initiatives, encouraging them to lead by example?	☐	☐	
Does the organization reward or recognize employees who demonstrate a commitment to watching for insider threats and upholding workplace cybersecurity measures?	☐	☐	

LEVERAGING ACCESS CONTROLS	YES	NO	COMMENTS
Does the organization follow the principle of least privilege by only giving employees and third-party collaborators access to the information and assets necessary to perform their job tasks or professional services?	☐	☐	
Has the organization implemented role-based access controls by periodically reviewing and updating individuals' account restrictions and privileges based on their current work assignments and responsibilities?	☐	☐	
Does the organization have effective privilege management protocols in place to ensure individuals don't abuse their access to company data and resources?	☐	☐	
Are employees and third-party collaborators required to keep their accounts secure by using multifactor authentication and creating strong passwords?	☐	☐	
Does the organization utilize network segmentation and segregation to limit the risk of insider threats moving laterally across its systems and compromising its entire IT infrastructure?	☐	☐	

UTILIZING THREAT MONITORING AND DETECTION SOLUTIONS	YES	NO	COMMENTS
Does the organization encourage employees to report any observations of suspicious activities among their co-workers and within company systems that may indicate insider threats? Are there specific reporting procedures in place?	☐	☐	
Does the organization leverage user entity and behavior analytics to identify abnormalities in account interactions and behaviors across its IT infrastructure?	☐	☐	
Does the organization use endpoint detection and response solutions to continuously monitor security-related threat information across its systems and technology and better detect and respond to insider events, particularly those involving malicious insiders and malware?	☐	☐	
Has the organization implemented email authentication technology to help keep dangerous emails (e.g., social engineering and phishing scams) out of potentially negligent employees' inboxes and limit the likelihood of them causing insider events?	☐	☐	
Does the organization use patch management solutions to keep security software up to date and reduce possible vulnerabilities for insider threats to exploit?	☐	☐	

SAFEGUARDING SENSITIVE DATA	YES	NO	COMMENTS
Has the organization categorized its data based on sensitivity and importance to help determine proper safeguards?	☐	☐	
Does the organization routinely back up critical data in a separate and secure location to maintain access to this information even when insider threats attempt to steal, damage or compromise the original copies?	☐	☐	
Does the organization encrypt sensitive data—both in transit and at rest—to limit the risk of insider threats exploiting critical company information, even if these individuals find a way to gain access to the locations in which such data is stored?	☐	☐	
Has the organization consulted legal counsel to ensure all data safeguards are compliant with applicable state, federal and international privacy laws?	☐	☐	

ENGAGING IN RESPONSE PLANNING AND MAKING CONTINUOUS IMPROVEMENTS	YES	NO	COMMENTS
Does the organization have a detailed cyber incident response plan that specifically addresses insider threat scenarios to help ensure a timely response and recovery following an attack?	☐	☐	
Does the organization run through the cyber incident response plan with its staff and evaluate the effectiveness of this plan through various practices (e.g., penetration testing and tabletop exercises), making updates as needed?	☐	☐	
Does the organization regularly assess its insider threat prevention and response policies and procedures and make improvements whenever necessary, such as when risks change or after insider events occur?	☐	☐	
Does the organization conduct post-incident analyses after insider events take place to investigate the incident's origin, determine overall losses, point out related cybersecurity weaknesses and make an effort to fill possible gaps with bolstered defenses?	☐	☐	
Does the organization utilize network segmentation and segregation to limit the risk of insider threats moving laterally across its systems and compromising its entire IT infrastructure?	☐	☐	

For additional risk management guidance, contact us today.

bch-insurance.com

This checklist is merely a guideline. It is neither meant to be exhaustive nor meant to be construed as legal advice. It does not address all potential compliance issues with federal, state or local standards. Consult your licensed commercial property and casualty representative at Brady, Chapman, Holland & Associates or legal counsel to address possible compliance requirements. © 2024 Zywave, Inc. All rights reserved.