Insider Risk Solutions

Managing Insider Risk

WHAT IS AN INSIDER THREAT?

In the wake of various high-profile leaks, human-enabled data breaches, and theft of corporate assets over the last several years, the "insider threat" topic has received much attention.

But what is an insider threat? An insider threat is a current or former employee, contractor, or vendor who has access to your organizations critical assets—customer records, confidential documents, intellectual property, physical assets, IT systems, or facilities—to commit malicious, negligent or inadvertent acts.

Malicious

An insider who intends to do harm to your organization and has a willful intent to steal information or sabotage systems, with a plan developed in advance.

Negligent

An insider who intentionally circumvents security controls assuming it will not have a negative impact on the business, and that no one will detect their behavior.

Inadvertent

An insider who unwittingly causes a breach or leak through unawareness or inattention.

Characteristics of "At-Risk" Insiders

Motivations can vary, but characteristics of a potential "at-risk" individual may include:

- ☑ Ethical flexibility
- ☑ Greed or financial distress
- ☑ Susceptibility to blackmail
- ☑ Intolerant of criticism
- ☑ Lack of empathy
- ☑ Self-entitlement
- ☑ Debilitating introversion
- ☑ Passive-aggressive
- ☑ Extreme compulsiveness

Potential Insider Risk Program Benefits

- Protect critical assets and prevent loss of intellectual and proprietary property, confidential data, or customer information
- Help determine if you align with applicable regulatory compliance, specifically for those in defense, healthcare, and financial services
- Avoid immediate or future loss of revenue
- Maintain customer and shareholder confidence
- Avert critical system or service availability disruption
- Prevent overall harm to an organization's brand image and reputation
- Deter potential insiders

A Shifting Threat Landscape

The global workforce has evolved. As retiring baby boomers leave the workforce, Generation-Y Millennials, raised on the internet and social networks, fill those gaps with the expectation – and even demand – for constant and immediate access to information, wherever they are on any and every device of their choice.

Generation-Y are accustomed to evolving technology, possessing greater levels of technical experience previously held primarily by engineers and IT professionals. They also have an increased expectation for connectedness and access.

Another factor, how simple it is to take anything stored electronically. Consider the volumes of sensitive data your organization has stored on your network. If a malicious insider wants to exfiltrate proprietary information from your network, it can be accomplished in a matter of minutes – if not less!

Finally, economic pressure. Certain nation states, companies and even people are in a financial crisis. Obtaining trade secrets and intellectual property can be used it to their economic advantage – selling it to the highest bidder and helping alleviate their financial stress.

As the workplace becomes more complex and insider risks increase, organizations must ensure they can detect anomalies and prevent incidents before they happen. This requires continuous monitoring, continuous evaluation of both human and IT-centric behavioral indicators and evaluation of individual attributes. Capgemini is your trusted partner to help protect your company's critical assets and help you prevent an insider incident before it occurs.

SAFEGUARDING YOUR MOST IMPORTANT ASSETS

Today's organizations often struggle to manage complex insider risk challenges independently. Although most cyber and risk professionals are well aware of the detrimental impacts an insider can have on their organization, many often lack the internal resources or expertise to develop a comprehensive insider risk management plan, or effectively respond to alleged or suspected insider activity.

Many corporations invest significant resources to improve their defenses against external threats but too often fail to adequately protect themselves from internal risks—risks created by insiders with direct access to critical corporate assets. Neutralizing internal threats is as important to strengthening overall security and reducing organizational risk as protecting against external attacks.

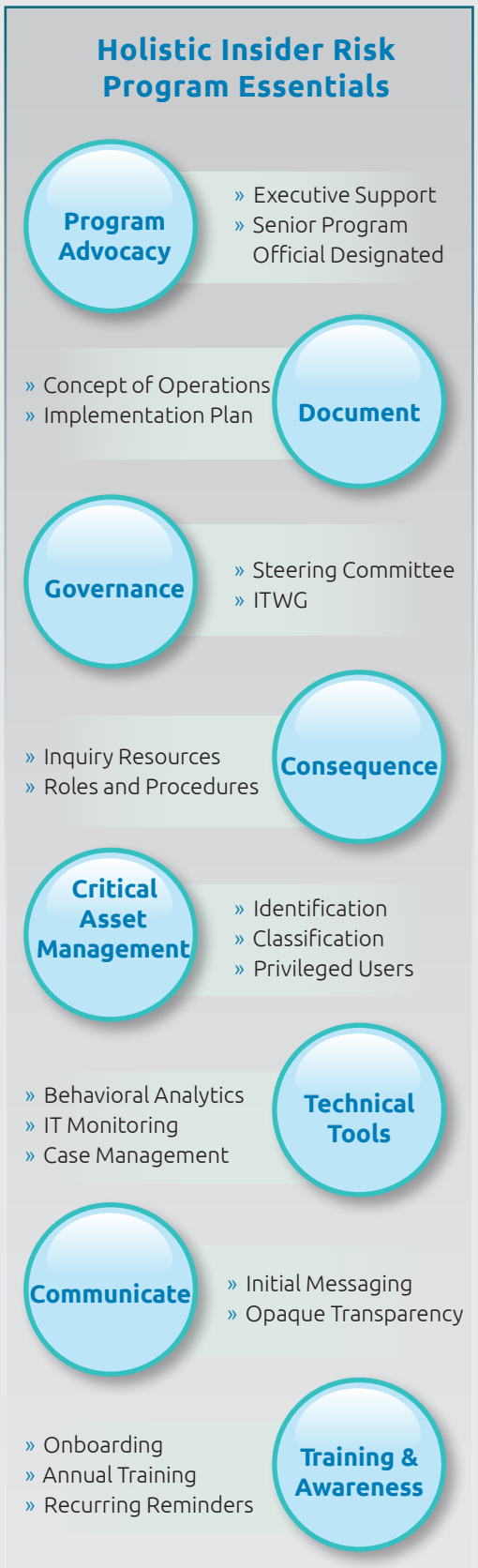
Are you confident your current insider risk program is comprehensive enough to protect your critical assets, and prevent loss of intellectual and proprietary property, confidential data, or customer information?

Can you effectively thwart an insider threat at your organization?

Are you willing to risk loss of revenue, customer or shareholder confidence, or harm to your organization's brand image and reputation?

Obstacles Launching an Insider Risk Program

- Convince executive leaders to invest in an insider risk program
- Create a powerful business case to fund and source the project properly
- Lack of internal resources or lack of the 'right' resources to build a strategic vision and deliver a holistic insider risk program
- Understand the essential components of an insider risk program
- Apprehensions employees will feel untrusted and that 'Big Brother' is watching
- Concerns over data privacy – especially for multinationals with stricter privacy laws or work councils (i.e. Europe)



CAPGEMINI'S APPROACH TO MANAGING INSIDER RISK

Providing a holistic, proactive, and risk-based approach through strong and effective policies, business processes, technical controls, and training.

Establishing a holistic, proactive insider risk program is essential to any organization that wants to manage insider risk effectively. However, many organizations think they need to attack the problem solely from a technical perspective and push it to the Chief Information Security Officer (CISO) or Chief Information Officer (CIO), but this may not be the most effective approach.

A comprehensive insider risk program requires people, processes, and tools, acting collectively to achieve the greatest benefit and return on investment. Therefore, Capgemini's preference is for the insider risk program to be led by a Chief Security Officer (CSO), or perhaps even the Chief Risk Officer (CRO).

When implementing an insider risk program, it is necessary to take foundational measures to integrate both technical and non-technical elements for a truly holistic defense. Some steps include constructing proper governance and documentation, defining critical assets vital to business operations, establishing processes for implementation and execution, and ensuring transparent communication with ongoing training for employees.

Our array of insider risk solutions and team of insider risk subject matter specialist are ready to assist you through all phases of assessing your current risk profile, creating and administering a comprehensive insider risk management program – including the recommended technology for your specific needs – and helping you to respond to insider incidents if they do occur properly.

CAPGEMINI INSIDER RISK SERVICES

Capgemini insider risk services can complement existing technical tools or may be employed independently, and include Insider Risk Assessment, Insider Risk Program Design and Implementation, and Insider Risk Investigative Response offerings.

Insider Risk Assessment

The Insider Risk Assessment evaluates and measures your organization's existing capabilities to help prevent, detect, and respond to insider threats by following a structured insider risk assessment process aligned with NIST, ISO, NISPOM, and other industry leading practices and standards. It includes a thorough review of administrative, technical, and physical controls that may be exploited by an insider to harm your organization and its critical assets, and provides a current state evaluation of your organization's insider risk security posture.

Generally scoped to a specific business unit and its operations, critical asset(s), or a specific type of insider activity, the assessment involves merging information from key stakeholders to form a comprehensive depiction of the company's level of preparedness to address insider-related threats.

Conducted by Capgemini's team of insider risk professionals, the assessment utilizes document reviews, direct observations, and personal interviews, including cross-functional areas of the business, to gain insight into organizational silos where relevant program information may reside. After each assessment, you will receive a detailed report that outlines the findings of your insider risk security posture, including risk treatment recommendations.

Insider Risk Program Design and Implementation

Capgemini will work with you to develop a vision for your insider risk program and initial framework to drive your program toward optimization. Our Insider Risk Program Design and Implementation Service is a natural next step following an Insider Risk Assessment (but can be offered independently). Once an assessment of your current state is complete, the desired goals for a successful insider risk program are defined and risk treatment recommendations identified, organizations use these actionable recommendations to design and implement a program.

WE LEVERAGE decades of counterintelligence, investigative, and industry experience

WE UNDERSTAND and evaluate current state to flush out vulnerabilities and improve risk program

WE MAKE informed decision makers on the most effective risk treatment recommendations and outline next steps

WE PROVIDE a comprehensive, holistic, and product agnostic view – not a rip and replace approach

WE DELIVER a valuable, actionable assessment

WE ARE your total insider solutions provider

INSIDER RISK CONSULTING SERVICES

Insider Risk "Quick Start"

Insider Risk Training

Insider Risk Assessment

Insider Risk Program Development

Insider Risk Investigative Response

Capgemini's team of insider risk professionals can augment your existing internal resources to design a holistic insider risk program that incorporates all the components for an effective program. Our consultants work with you to develop or modify relevant business processes, organizational policies, and security awareness training, as well as integrate appropriate technology to enable your organization to counter threats while minimizing business disruption.

Insider Risk Investigative Response

When there is concern of potential insider activity within your organization, Capgemini works with you to resolve the matter successfully. The Investigative Response Service is customized to your organization's specific needs but typically involves our consultants working with you to develop an investigative plan, gather facts, collect evidence, and guide the investigation's detailed day-to-day execution related to the insider incident.

Capgemini in-house analytical resources and highly-skilled cyber forensic professionals can support the needs of any investigative effort. Our subject matter practitioners leverage their decades of counterintelligence and forensic investigation experience to help you assess anomalies and other indicators of insider threats and respond accordingly. Each team member keenly understands the sensitivity of internal investigations and can be trusted to maintain the highest level of discretion.

THE TECHNOLOGY

Traditionally, organizations believe that network monitoring tools were sufficient to detect an insider threat. But network monitoring only captures the individuals' virtual data or digital trail – what systems an individual accesses, when they view and download files, send emails, access the web, and log on and off the corporate network. Many times these activities are not found early enough or simply not identified at all.

Organizations must also take into account non-virtual risk indicators to develop a proactive and effective insider risk program. For example, the individuals' role, access and clearance levels, work habits (i.e. what hours do they 'normally' start/stop work), compliance to corporate policies, and even their performance rating (have they received a reprimand, are they at risk for termination).

Arena Insider Threat Identification™

The Arena ITI™ solution is designed to provide organizations of any size with proactive identification of potential insider threat activity, built on industry-leading experience in counterintelligence.

This award-winning solution takes a holistic approach to detecting insider threats, integrating structured and unstructured contextual information, such as performance reviews or employee information access, as well as data from cyber monitoring applications to provide a robust and effective insider threat detection solution.

Arena ITI analyzes individuals' anomalous IT activities with their non-IT behaviors in a single platform to produce faster, highly accurate, insider threat detection by:

- Continuously ingesting intelligence from disparate company data sources
- Aggregating data through predefined models and scoring
- Drilling down for advanced analysis and further investigation

To complement the advanced Capgemini Arena ITI data and analytic models, Capgemini also offers clients a solution for User and Entity Behavior Analytics (UEBA). UEBA software integrates raw log type data sources and analyzes unusual behavior using machine learning models. UEBA software is designed to provide a clear picture of threats across IT systems by tracking the relationship between, and risks associated with, users, machines, applications, and files. When Arena ITI™ is complemented with a UEBA application, it offers clients the most robust insider threat solution available.

Can your organization correlate this virtual and non-virtual data?

More importantly, if for example, an individual downloaded a large number of proprietary files, outside of their normal working hours, and also had just received a poor performance review, would this collective activity generate an alert and trigger an internal analyst to take a closer look at that individual?

WHY PARTNER WITH CAPGEMINI?

Our Defender DNA

Successful cyber programs require great people with 'defender DNA.' Defending against sophisticated cyber threats takes more than technology. It takes people. People with skills and innate qualities to outpace today's evolving threat landscape. Qualities we call "defender DNA." We see these qualities in successful client teams and in our own team.

Our consultants leverage their defender DNA. Their many years of counterintelligence, investigative, and industry experience help our customers develop, implement and manage an end-to-end, holistic, insider risk program.

Organizations across both government and private sectors as well as multiple industries rely on our team to help them understand and evaluate their current state, flush out vulnerabilities and gaps, develop their strategic vision, evaluate which technology is best suited to their needs, and design and implement their insider risk solution.

Our experience of insider risk program leading practices will help inform and influence your decision makers on the most effective risk treatment recommendations and include the enhanced risk treatment solutions for your organization. We provide a comprehensive, holistic, and product agnostic view.

Capgemini is a total insider solutions provider, coupling an entire suite of cyber products to address technical insider threat issues.

NEXT STEPS:

Don't wait to be a victim of an insider threat. Find out how your organization measures up, what steps you can take to improve your insider risk profile, and how to respond when an incident occurs. Talk to a cybersecurity professional today.

TRUST CAPGEMINI TO HELP SAFEGUARD YOUR MOST IMPORTANT ASSETS.

About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Learn more about us at

www.capgemini.com/cyber

People matter, results count.

Capgemini

CSNA.19.06.03.L023.R02