CISO COUNCIL SERIES: BUILDING AN EFFECTIVE INSIDER THREAT PROGRAM

A special publication from Ping Identity's CISO Advisory Council

WHITE PAPER

TABLE OF CONTENTS

03 Introduction

04 Step 1: Form the Core Team to Own Your Insider Threat Program

05 Step 2: Develop Your Insider Threat Model

06 Step 3: Identify the Critical Roles to Watch

07 Step 4: Specify Process & Technology Needs

09 Using Technology to Prevent Insider Threats

INTRODUCTION

Ping Identity's CISO Advisory Council is comprised of CISOs and security leaders from enterprise organizations, including: Chris Gullett, VP of Information Security for Allegiant Air; Krizi Trivisani, CISO for American Red Cross; Diane Ball, CISO for BCBS Tennessee; Harshal Mehta, CISO for Carlson Wagonlit; Karl Mattson, CISO for City National Bank; Sam Masiello, CISO for Gates Corporation; Michael Strong, CISO for GCI; Rich Gay, CISO for PowerSchool Group LLC; Mark Freed, CISO for TechnipFMC; Adrian Mayers, CISO for Vertafore; and Greig Arnold, CISO for Vista Consulting Group.

Insider threats are a well-known problem—and one that few enterprises are immune to. An Insider Threat Report from Crowd Research Partners found that 90% of organizations feel vulnerable to insider attacks, while 53% confirmed they'd experienced insider attacks against their organizations in the previous 12 months.[1]

Unfortunately, detecting insider attacks in time to minimize their impact grows more complex every day. Because insiders can be anyone who at some point was granted access to sensitive systems and data, the potential attack surface is broad. This means that current and former employees, as well as business partners and contractors represent potential vulnerabilities.

34%
of attacks involve inside actors[2]

Expansion of the insider threat surface is further driven by digital transformation initiatives, which increasingly provide access to sensitive information across resources deployed inside and outside the corporate data center. Adding to the complexity, the threats you face can come in many forms and with varying degrees of impact, from the incidental and innocent to the well-planned and malicious.

While building an effective insider threat program might feel like a daunting task for those who have yet to do it, you'll find four simple steps to get you off on the right foot in the pages that follow. Even if you already have an insider threat program in place, you can reference this paper when reviewing your current program to determine if updates or additions may be worthwhile.

STEP 1: FORM THE CORE TEAM TO OWN YOUR INSIDER THREAT PROGRAM

The most successful insider threat programs are multi-disciplinary efforts. Input into the program's design and requirements—as well as enforcement of the program's principles—takes a village. There are three departments within an enterprise that are commonly involved in program design and ongoing management. It's critical that these teams work together, while coming to a consensus on who is the official program owner and who is providing support.

Security & Risk

Knowledge of where sensitive data resides, who has access to it and under what circumstances is the domain of security professionals. Also under the security and risk umbrella is knowledge of the common ways insiders abuse their privileges, existing controls to prevent this abuse and which tools provide them. Security teams with an emphasis on insider threats also continuously monitor the commercial and open source landscape for new ways to detect and prevent breaches from insiders.

Human Resources (HR)

Preventing an insider breach starts well before an individual is permitted to access sensitive data and continues after this access is terminated. The processes which contribute to prevention are often intertwined with onboarding and offboarding procedures, typically owned and managed by HR departments. When an insider commits a violation, your HR team will be involved in determining and applying the appropriate disciplinary response. From pre-employment screens to ongoing enablement and exit precautions, HR plays a key role in carrying out enforcement of insider threat programs.

Legal

While legal departments usually don't actively mitigate insider risk, they often define the boundaries of what does and doesn't constitute malicious intent. For example, legal departments take great care in defining thresholds for intentful and incidental data theft, as well as determining the specific consequences of actions which meet those criteria. After all, there can be significant differences in both the intent and impact of a breach depending upon the situation. For example, accidentally sharing data with a trusted partner is very different from a salesperson exiting with a list of customers or a developer sabotaging an internal system.

STEP 2: DEVELOP YOUR INSIDER THREAT MODEL

The creation of an insider threat model is similar to other threat modeling exercises. It starts with a discussion of the threats you're most concerned about, as well as those you can reasonably address.

Some potential risks of an insider breach include:

- Leaking of organizational critical assets
- Leaking of personal data and information
- Modification or theft of confidential or sensitive information for personal gain
- Sabotage of the organization's data, systems or networks
- Theft of trade secrets or customer information to be used for business advantage
- Sharing of trade secrets or customer information with a foreign government or organization
- National security espionage

The threats you face will be dependent upon your organization and the nature of your business. For many, preventing the theft of sales-related data or intellectual property is a common concern, while uncovering potential sabotage by an undercover state actor is not as typical. The risks you need to address should be ranked, and your organizational focus should be adjusted accordingly.

STEP 3: IDENTIFY THE CRITICAL ROLES TO WATCH

Development of a successful insider threat program is not a one-size-fits-all initiative, but there are some core elements you'll want to include. One of them is applying monitoring and preventative controls that are risk appropriate on a per-role basis. Based on the results of your threat model, you should be able to identify those departments and teams that are at the highest risk of insider threat.

While some of these roles will be organizationally specific, there are others that pose a high risk in nearly all organizations. For example, sales, finance and executive leadership are typically a focus of insider threat programs because of their day-to-day access to sensitive information like customer lists, financial performance data and IP. Those in your organization with knowledge of security processes and procedures, such as system administrators, as well as fraud-focused roles should also be included.

Aside from these fairly obvious targets, you also want to consider others who may pose vulnerabilities. Three roles that are often overlooked but deserve your attention include:

- **Third Parties:** Privileged third parties can provide insider access and should be considered as a part of your insider threat program.
- **Customer Service Agents:** Customer service personnel often have access to personally identifiable information (PII) for knowledge-based authentication and other purposes, meaning account-level data is also accessible by this audience.
- **Developers:** Software developers present a similar risk to systems administrators in that they can leave backdoors open in sensitive resources to later leverage.

Prioritizing these roles can be difficult, but it's worth some time and effort. Doing so can guide you to the appropriate level of detection and introspection processes and capabilities required for each audience.

STEP 4: SPECIFY PROCESS & TECHNOLOGY NEEDS

When thinking of the controls needed to prevent insider breaches, you want to cover all of your bases. Approaching it from a lifecycle perspective is a good way to ensure you identify the various controls you can apply at each stage, including before people are given access (generally pre-employment), while they have access (during most of their employment) and when access is terminated (generally during employee off-boarding).

Before Access is Granted

Before you grant access, your goal is to filter out candidates who are more likely to act maliciously in your environment. While reference checks are common, they can be problematic due to the limitations on what previous employers are able to disclose. Backchanneling through alternate contacts to do less formal reference checks on high-risk hires can be quite effective but the practice doesn't scale well.

To gain a higher level of assurance, conducting pre-employment screens such as criminal and educational background checks are recommended. You can take this further by assessing other dimensions such as conflicts of interest, financial history and drug tests. The use of hiring processes like employee non-compete and confidentiality agreements and code of conduct policies can provide an additional layer of protection, while also establishing clear guidelines and expectations with new users.

While Access is Available

During the period where access is available, HR and Security teams typically work together using a combination of process and technology to mitigate insider threats. Awareness and training on acceptable use and security best practices are critically important for setting expectations. You want to give insiders clear and consistent guidelines for securing corporate data while also ensuring awareness of non-compete and confidentiality policies. Training is also an ongoing concern, so reiterating your policies and expectations regularly is necessary.

In addition to training, technology plays a critical role in the prevention, detection and mitigation of insider threats, regardless of the intentions of the actor. Some common ways to use technology to reduce insider threats include:

- Strong authentication and authorization
- Cloud access security brokers
- Unified endpoint management/enterprise mobility management
- Endpoint detection and response
- Data loss prevention
- Digital rights management
- User entity and behavioral analytics
- Deception technologies

It's equally important to understand how you can apply these technologies across a broad range of technology types. On-premises systems, IaaS/PaaS (infrastructure/platform as a service) and SaaS environments each offer unique challenges when it comes to applying your technical controls, and each will have discrete requirements. Generally, you will have much fewer options when working in a SaaS environment, but have complete flexibility in your own data center.

After Access is Terminated

Removing access to sensitive data is perhaps the most important part of an insider threat program, as employees are most likely to steal data when they're leaving your organization. A survey by Osterman Research found that 69 percent of organizations have suffered significant data or knowledge loss from employees taking information resources with them when they left the business.[3]

You also want to understand the nature of the employee's departure and their next career move. Both voluntary and involuntary terminations present risks. If the employee was released involuntarily, they may have a grudge to settle. Even if an employee is leaving voluntarily, they may be taking a new job with a competitor.

Employees most often take contact lists, price lists and marketing materials. And in many cases, the employee may not think they're being malicious.[4]

If the employee is headed to a rival organization, you'll want to review the employee's recent behavior, including the data they've accessed, and compare it to their typical past behavior and peer behavior to see if there have been changes. You'll also want to look at their history well before when they gave notice. Employees may begin taking data 60-90 days before they ever notify the company that they're leaving, so don't overlook this potential.

USING TECHNOLOGY TO PREVENT INSIDER THREATS

Automating the detection of insider (and other) threats will become more common as artificial intelligence (AI) and machine learning algorithms become pervasive across a broad range of security tools. These tools will continuously provide attributes to establish a risk score tied to a specific individual, enabling just-in-time and just-enough access through intelligent authorization and continuous recertification.

> “Track insider behavior by monitoring and logging access to sensitive data.[5]”

Killing the password will also contribute greatly to preventing breaches that begin with credential theft. Credentials are often compromised due to employees and third parties reusing passwords across work related and non-work related online services.

Removing passwords altogether will shrink the ways non-insiders take advantage of the poor security hygiene practices of insiders, especially those from third parties over which enterprises have little to no control. FIDO2 and other identity standards are rapidly gaining adoption to support this reality. Adopting services which support these standards will help your organization remove compromised credentials from the threat equation faster.

As technology changes and evolves, you can also expect new solutions to enter the market that will provide additional threat insights and protection. Three areas of concern that are ripe for innovation include:

- **Gaps in the Shared Responsibility Model:** Cloud providers (SaaS/PaaS/IaaS) don’t always provide the tools or allow you to bring your own to support a standardized insider threat program.
- **Complications Introduced by TLS 1.3:** TLS 1.3 makes network-based decryption difficult or impossible. This will increasingly make network-based approaches to DLP challenging.
- **Bring Your Own Device (BYOD):** The continual push to improve employee performance and productivity will mean more users working from their personal devices. This makes monitoring and mitigation much more difficult.

Your insider threat program must be nimble and flexible to take advantage of new defense measures and respond to changing risks. This includes conducting regular reviews of what's working well and what you could be doing better, as well as staying abreast of the latest research and developments in insider threat detection and prevention.

About Ping's CISO Advisory Council

Made up of CISOs from leading global enterprises, this group provides insight to Ping Identity on security, privacy and compliance challenges within the global enterprises we serve. It helps inform Ping's strategic vision, product roadmap and go-to-market strategies. Interested in getting involved? Please reach out to your account executive to learn more.

1 Insider Threat 2018 Report, Crowd Research Partners.
2 2019 Data Breach Investigations Report, Verizon.
3 Patrizio, Andy, "Sensitive data often follows former employees out the door," CIO, Apr 27, 2017.
4 Ibid.
5 2019 Data Breach Investigations Report, Verizon.