WHITE PAPER

THE IMPORTANCE OF CONTINUOUS EMPLOYMENT SCREENING IN APAC

Cisive

It is commonplace for regulated institutions and industries in Asia to perform initial background screening checks on their new hires to identify red flags in their work experience, credentials, legal documents or financial history. The problem with adopting this one-time approach is that it merely enables verification of such data during a moment in time.

Keeping up to date about an employees' background is as important as verifying the candidates' data when they initially apply, especially as this data is not static. If an employee commits a crime, has a license revoked or loses work authorization after being hired, an employer may come to never find out and may face potentially damaging risks to their reputation as a result of an employees' actions. This is particularly important for high-risk industries with access to vulnerable people, or where direct consumer access or storing information of a highly sensitive nature is required within a firms' scope of work.

The 2020 Data Threat Report (Asia Pacific Edition) by Thales found that 47% of respondents (consisting of APAC executives from 8 different countries) had experienced a data breach throughout their careers; with 27% of data breaches occurring solely in 2019, and that 18% of Asia Pacific organizations admitted to failing a compliance audit within the same year. The report also uncovered that an overwhelming 69% of respondents stated cybercrime was their highest concern in the midst of the COVID-19 era that poses new and emerging risks to companies.

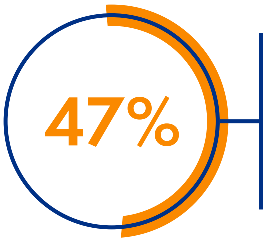
Adopting continuous monitoring practices such as rescreening can effectively assist organizations in APAC through providing them with a risk mitigation system and enabling HR, hiring managers or a company's leadership team with a proactive approach in complying with the latest local and global regulations and recommendations.

Understanding Insider Threat

WHAT ARE INSIDER THREATS?

An insider threat occurs when someone close to the organization with authorized access misuses that access to negatively impact the organization's critical information or systems. An insider does not necessarily or solely refer to an employee; as third party vendors, contractors and partners can also pose a threat to companies. Insider attacks can be committed by virtually anyone that has access to Personally Identifiable Information (PII), is aware of the policies, systems and controls used in an organization, or has gained access to an organization's vulnerability, such as their loosely enforced policies and exploitable IT systems or networks.

Findings from the Ponemon Institute's 2020 Cost of Insider Threats Global Report found a staggering **47% increase in the number of global insider threat-related occurrences from 2018 to 2020**; and that the overall costs that derived from insider related incidents had similarly risen across the globe. To illustrate, a 31% increase of insider-attack related costs occurred during 2018 to 2020, rising from USD $8.76 million in 2018 to $11.45 million in 2020. In Asia-Pacific alone, the total annualized activity cost spent by companies that experienced insider related issues amounted to USD $7.89 million.



Increase in the Number of Global Insider Threat-Related Occurrences from 2018 to 2020

The global report also assessed the percentage distribution of insider-related incidents based on the average time taken for companies to contain them; and concluded that the average time was a lengthy 77 days. This data suggests that insider threats are becoming increasingly rampant across APAC, and that it is still an under addressed issue that poses malicious risks such as fraud, information theft and IT-network sabotage.

Many Asia-Pacific companies have developed cognitive dissonance regarding data security and organizational risk; despite the recent increase of insider related incidents and costs, 52% of APAC executives state they are very or extremely secure (2020 Thales Data Report). When considering perceptions on employee screening processes in APAC, many employers develop a false sense of security after complying with standard hiring measures; such as relying on the pre-employment background check of their new hire as a means of ensuring safety throughout the course of their employment.

While upfront screenings are essential in making educated hiring decisions for the business, a single screening process alone is not sufficient in guaranteeing a consistently risk-free workforce. Depending solely on background screening information acquired during the hiring process only provides a snapshot of an employee's relevant history prior to joining a company. Rescreening current employees can highlight important changes that organizations should remain aware of, such as an employee's continued qualifications for their existing role or inappropriate content they may be publishing online.

Adopting a rescreening approach in monitoring employees can help keep companies safer from fraud, theft, and reputational damage. It additionally reduces the risk of a company's employees, clients and the broader public being exploited by malicious actors.

Driving Factors

Understanding the nature of these 'attacks' can help firms identify risks easier and garner knowledge about the potential motivations behind threats posed by their internal workers. Determining the root causes behind insider related incidents additionally serves as a medium that companies should consider when implementing risk mitigation policies and procedures. To minimize risk, companies can adopt best practices such as employee rescreening, developing employee awareness programs, and adopting advanced information security policies in the current day.

WORK-FROM-HOME (WFH) MEASURES

The ability to proactively detect, evaluate and mitigate workforce risk by understanding all risk factors is critical in safeguarding businesses from emerging risks due to the ongoing pandemic. COVID-19 has shown work-from-home (WFH) to be a viable model for companies. In consideration of this, more employees may demand access to similar flexibility in the future, and more organizations may adapt to offer it. However, appropriately adjusting to the ongoing development of different WFH models may also pose greater challenges to businesses; namely in terms of greater data and security threat exposure deriving from concerns about employees working alone at home and using devices that do not enable forms of supervision. In this instance, malicious actors can exploit such loopholes to their benefit and can easily commit crimes within the organization they work for.

As the WFH model is a fairly new process, many companies may not have existing measures in place that can stop employees from transferring data to their private thumb drives or taking photographs of their screens with their mobile phones and other devices. Due to the complexities of WFH frameworks and measures, illegally copying data without the company knowing is one of the many data breaches an employee can easily execute, alongside other opportunities to commit fraud or misconduct.

In the age of COVID-19, additional risks posed by employees can be accredited to motivations such as:

- **Increased financial needs** for management that are facing pressure to meet key financial targets or employees who may have taken a pay cut;
- **Opportunities** for fraud given the internal controls of the organization may have changed recently to adapt to working from home; and
- **Rationalization** of employees who might be afraid of losing their jobs despite having been committed employees.

TRENDS ON INSIDER RELATED THREATS IN APAC

Alongside factors pertaining to the global pandemic, it is important to consider additional trends to assess all elements and form a cohesive picture for APAC businesses to understand how rescreening practices are essential in mitigating such threats. The 2019 APAC Cybersecurity Survey by SolarWinds determined that the top threat challenge across 101 companies in Singapore and Hong Kong were related to security incidents, with the root cause of such incidents pertaining to the following:

- 66% of respondents cited regular employees as the main committers for one or more insider related incidents; and
- 53% of respondents cited privileged IT admins as the main culprits.

The findings from the 2019 APAC Cybersecurity Survey highlight an increasing need for companies in Asia Pacific to implement preventive security best practices such as rescreening. Adopting this approach will help firms move from a reactive to proactive workforce and safeguard them by utilizing systems that look holistically and periodically across the entire enterprise.

Case Studies

An arrest made during 2020 in Singapore revealed how a former bank relationship manager of a global bank had forged numerous signatures and bank documents, deceived the bank by transferring SGD $10,000,000 to a third party account to pay off his debts, and engaged in numerous unauthorized stock and foreign exchange trades that totaled to a net loss of USD 10 million to the bank (Monetary Authority of Singapore, 2020). As a result of his actions, he was sentenced to 13 years' imprisonment, convicted of forgery and convicted of cheating under the Penal Code ("PC") and of offences under the Computer Misuse Act. **Moreover, the 2 prohibition orders (PO) issued against the former bank employee included:**

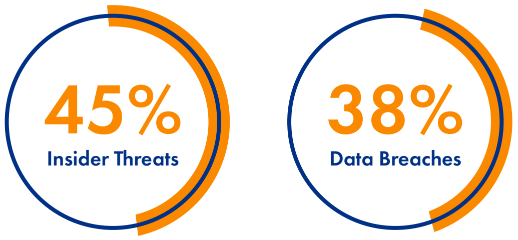
(i) Prohibition for a period of 25 years from (i) providing any financial advisory service, taking part in the management of, acting as a director of, or becoming a substantial shareholder of any financial advisory firm under the Financial Advisers Act (Cap. 110) (FAA); and

(ii) Performing any regulated activity, or taking part in the management of, acting as a director of, or becoming a substantial shareholder of any capital market licensee under the Securities and Futures Act (Cap. 289) (SFA).

Another case relating to insider incidents is the the Pakistan International Airlines (PIA) incident, where PIA dismissed 63 employees; including 33 members of staff that used fake credentials or licenses to help attain their current job positions in the company. As the number of insider related cases rise in Asia, the risks posed by insiders within APAC companies are increasingly apparent and is a rising threat that organizations need to identify and mitigate.

Adobe's 2020 CIO Perspectives Survey revealed an astounding 89% of CIOs in India and Australia agree to placing greater importance on cybersecurity issues and re-asserted that cyber security continues to be one of the most cited areas for planned investment, both prior to COVID-19 and during the current climate. **Specifically, some of the most prominent areas of cybersecurity related issues for Indian organizations were pertaining to insider threats (45%) and data breaches (38%).**

Most Prominent Cybersecurity Related Issues for Indian Organizations



The emerging amount of various research reports and cases should read as a warning sign for organizations in APAC: it is imperative that more companies in Asia establish clearly defined best practices such as rescreening, as well as adopt up-to-date data and security measures.

Best Practices

Adopting the following best practices are vital in helping companies in Asia prevent insider threats and minimize the risk of sensitive data being compromised:

(i) Establish clearly defined security policies and procedures;

(ii) Maintain consistent enforcement, documentation and review of regular policy, data security policy and employee policy training; and

(iii) Create appropriate parameters for screening applicants and checking facts against the most recent public records available.

ASSESSMENT OF EMPLOYEES

Understanding your critical assets, their vulnerabilities and the potential threats they may pose can primarily be assessed through rescreening employees. Record files of employees from their pre-employment screening background checks may no longer be updated, especially as data points are likely to change over time; such as:

- Criminal checks;
- Financial checks;
- Credit reports;
- Bankruptcy checks;
- Civil litigation checks; and
- Social media and adverse media searches.

WHEN TO CONDUCT RESCREENING?

Unless a company has existing continuous monitoring practices set in place, they will not be protected against any new risks that may emerge. In consideration of this, APAC companies should adopt rescreening practices regardless of preexisting concerns or incidents, as it acts as a security and prevention measure. In considering when to conduct rescreening, the following is recommended:

(i) Rescreen current employees or volunteers **upon promotion** or changes to job responsibilities and positions;

(ii) **Rescreen contractual workers** every time they're hired for a new project;

(iii) Rescreen employees **after being involved in a suspicious workplace incident**; and

(iv) Rescreen your organization's **leadership team**, including all **board members**.

INTERNATIONAL BACKGROUND CHECKS

1. **Records and processes differ from country to country**
   - Consider that access to public records can vary depending on region. For example, there are currently no centralized databases in Indonesia from which to retrieve comprehensive information on individual criminal records; thus any criminal clearance from either police or courts may not be reliable.
   - Collect country and search-specific consent forms from your applicants.
   - As records may be presented in local languages, ensure your provider can accurately translate and interpret the records returned.

- Background checks can be time consuming, thus proper time management and organization skills should be exercised to verify details before the candidate's start date.

2. **Legal and legislative concerns**
   - Ensure you're educated on labor law protections, as well as work councils, data privacy and protection.
   - Confirm that your provider understands data localization – especially when it comes to countries like China, Japan or Korea as their data privacy and protection laws are more strict.
   - Verify that your background screening partner is following the respective Asian country laws, GDPR and US privacy regulations.

Developing an Employee Awareness Program

One of the key ways companies in Asia can effectively ensure a safe and motivated workforce and retain talent is implementing effective employee awareness programs. Not all insider related incidents are as easy to identify as an employee using a fake certificate or embellishing their resume. Unscrupulous staff will operate in any grey areas they find, such as the case of the former bank relationship manager in Singapore that committed numerous crimes over a lengthy period of time. In this regard, there is a crucial responsibility to act quickly and mitigate any internal risks that may damage the reputation and culture of safety and security within an organization.

Building an employee awareness program helps companies by eliminating grey areas, uncovering potential trails of evidence more easily and conveying full transparency to employees **about what is and what is not acceptable according to the terms set by the organization and according to the regulations within the specific jurisdiction.** An employee awareness program should be enterprise-wide and establish clearly defined criteria; including roles and responsibilities for preventing, detecting, and responding to insider behavior or insider related incidents.

Upon proved incidents or suspicion of threats, legal counsel is vital during the information-gathering process to ensure all evidence is gathered and maintained in accordance with legal standards and that a prompt legal response will be issued when necessary. Legal counsel should also ensure that information is shared properly among the insider threat team members, for instance, to ensure the lawful privacy of employees' mental and physical health information. Having a guideline at hand can additionally serve to lower risks of an insider deciding to harm the organization through informing employees on the consequences of carrying out offences; such as outlining how committing a data breach will result in immediate termination.

Key Takeaways

DEVELOPING AN ACTIVE EMPLOYEE AWARENESS PROGRAM INCLUDES:

- Establishing stringent access controls and monitoring policies on privileged users;
- Monitoring all remote transactions and ensure that remote access is disabled during employee termination (in accordance to the law within the specified region);
- Implementing strict password and account management policies and practices;
- Conducting consistent and enterprise-wide periodic training on security policies and procedures;
- Creating a swift response plan in the event an insider does harm the organization; and
- Creating an anonymous employee reporting program (such as a hotline) regarding indicators such as suspicious or disruptive behavior, financial concerns, suspicious travel or suspicious contacts.

It should be noted that what people constitute as indicating factors of insider threat can vary based on location and culture. For instance, tardiness at work or missed project deadlines may indicate an opposing correlation to insider threat in Western cultures, which view time as adjusted to suit the needs and roles of the people, as opposed to monochronic cultures, which place a high importance on following schedules and may deem lateness as suspicious behavior. Thus, consideration of culture should also be assessed when developing an employee awareness program, as well as in implementing insider threat related best practices or when training employees.

ABOUT CISIVE

At Cisive, we are experts in the specific risks and regulations that apply to the financial services and other highly regulated industries. For many years, we have provided tailored solutions to meet the unique requirements of our enterprise clients.

Cisive's service model provides a single, integrated system throughout the globe using complete applicant information and country-specific forms. Cisive returns information to our clients through a centralized system for analysis, quality control, presentation, and billing.

With over 4 decades of experience and expertise in working with many of the world's largest financial services institutions, Cisive's deep insight into employment screening practices and industry knowhow, is unlike any other background screening provider in the industry.

Your business will not only get a background screening provider, but a lifelong partner – a company that stands by their work; protects their clients and provides the consultation and guidance world class act organizations are looking for.

CONTACT US

🌐 www.cisive.com

✉ info@cisive.com

☎ 866.557.5984

Cisive