



## The rise of insider threats amid COVID-19

A weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.

### Inside threat actors are exploiting vulnerabilities

The COVID-19 pandemic has sparked massive workforce transformation. As noted in past weeks, the unprecedented transition of countless employees, contractors, and third parties to remote work has left many organizations unprepared to monitor or detect insider threats that may arise due to unauthorized remote access, the misuse of personal devices, mounting reliance on cloud infrastructure, weak password and authentication policies, unsecure networks and printing equipment and misuse of corporate assets. Just as critically, however, the turbulence created by COVID-19 is proving fertile ground for malicious insiders. Because insiders are uniquely placed to circumvent perimeter network monitoring and expose an organization's security vulnerabilities, these incidents can be particularly devastating. In fact, the average cost of insider threats catapulted by over 30 percent in the past two years, to \$11.45 million annually. This week we highlight the growing risk of malicious insider threats.

**92%** of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor

**59%** of employees who leave an organization voluntarily or involuntarily say they take sensitive data with them

#### Threat actor recruits insider to access personal user data – Impact reach: All | Geographies: Global

On May 4, 2020, news media outlet Vice reported that an unidentified threat actor bribed a Roblox employee to gain access to a back-end customer support panel of the popular online video game. The access enabled the threat actor to potentially view the personal information of over 100 million users, and to possibly change passwords and disable two-factor account authentication. The threat actor first paid an insider to perform user data lookups for them, and then separately targeted a customer support representative via phishing. The targeted employees appear to have been identified through their LinkedIn profiles.

#### Terminated employee disrupts delivery of medical supplies – Impact reach: All | Geographies: Global

On April 16, 2020, a former employee of a medical device packaging company was charged by the U.S. Department of Justice for conducting a computer intrusion into his former employer's shipping system, disrupting the delivery of personal protective equipment (PPE) to healthcare providers. While employed, the accused had administrator access to the company's shipping systems. The intrusion took place following the accused's termination and just three days after he received his final paycheck. Using a fake account he'd created while employed, the accused allegedly edited over 115,580 records and deleted another 2,371, before the fake user account was deactivated.

### Be Aware: types of insider threats

An insider is a person who has the potential to harm an organization for which they have inside knowledge or access. An insider threat can have a negative impact on any aspect of an organization, including employee and/or public safety, reputation, operations, finances, national security, and mission continuity.



→ Predicated to be most prevalent during COVID-19

#### These threats can be realized through:

- Malicious intent**  
*Intentionally abuse a trusted position and access to inflict damage for financial or personal gain*
- Ignorance**  
*Lack of awareness and understanding of their security responsibilities*
- Complacency**  
*Take a lax approach to security, contrary to organizational expectations*



Although most insider threats are caused through negligent behavior, the turmoil caused by COVID-19 presents inside threat actors with a prime opportunity to abuse their account privileges and/or technical knowledge to exfiltrate sensitive data, commit fraud, or sabotage business operations. Based on observed activity and public disclosures, Deloitte CTI assesses with high confidence that malicious insider threats are rising.

Here are some ways to counter the threats:

**Identify high-risk insiders.** Typically, the majority of malicious insiders are high-risk individuals who have recently been terminated or furloughed, have a history of IT policy violations, have requested undue access, or who are otherwise disgruntled. However, during this pandemic, organizations should be aware that the impact of COVID-19 could create stressful, desperate, even opportunistic, situations for employees who previously may not have considered such activity. Keep in mind, too, that an insider can be an employee, a contractor, or a vendor that uses their verified access to commit a malicious act. It is important to identify potential risk indicators from various parts of the enterprise (e.g. HR, Whistleblower line, Cyber, Fraud, etc.) and consolidate them to proactively identify potential employees who may turn in to insider threats.

**Stay a step ahead.** Insiders' methods, tactics, and attempts to cover their tracks will constantly evolve, which means your insider threat program and the precursors it analyzes should continuously evolve as well. This can be achieved through a feedback mechanism that includes an analysis of ongoing and historical cases and investigations.

**Limit access.** Follow the principles of least privilege by providing employees with the most limited system access they require based on their role and duties.



**Trust but verify.** Maintain an accurate inventory for computers, mobile devices, and removable media, and conduct routine and random audits to keep track of your assets.

**Look for anomalies.** According to the FBI's Insider Threat Program, detection of insider threats should use behavioral-based techniques. Consider implementing a user behavior analysis (UBA) tool capable of monitoring user activity and flagging anomalous behavior.

**Monitor insider threat indicators.** Organizations may find individuals experiencing insecurity and stress over the fear of losing a job during this time of COVID-19 and may attempt to "protect themselves" through actions that are proactively malicious. By implementing mobile and cloud security solutions, such as a cloud access security broker (CASB)—a tool to help enforce your security policies when your resources are accessed in the cloud—you can begin to identify potential risk indicators and high-risk behaviors exhibited by remote employees. This can be used to identify insider threats and shed light on weak or missing processes.

Deloitte China Cyber Risk Partners



**Xue, Tony**  
National Cyber Risk Leader  
Tel: +86 10 8520 7315  
Email: tonxue@deloitte.com.cn



**Jiang, David Wei**  
Eastern Region  
Tel: +86 21 2312 7088  
Email: davidjiang@deloitte.com.cn



**He, Tommy Xiaoming**  
Northern Region  
Tel: +86 10 8512 5312  
Email: the@deloitte.com.cn



**Kwok, Eva Yee Ngar**  
Southern Region, Hong Kong  
Tel: +852 2852 6304  
Email: evakwok@deloitte.com.hk



**Feng, Steven Ye**  
Eastern Region  
Tel: +86 21 6141 1575  
Email: stefeng@deloitte.com.cn



**Shih, Nathan Pei-en**  
Eastern Region  
Tel: +86 21 3313 8366  
Email: nathanshih@deloitte.com.cn



**Xiao, Frank Tengfei**  
Northern Region  
Tel: +86 10 8512 5858  
Email: frankxiao@deloitte.com.cn



**Pihkanen, Miro**  
Southern Region, Hong Kong  
Tel: +852 2852 6778  
Email: miropihkanen@deloitte.com.hk



**Kukreja, Puneet**  
Eastern Region  
Tel: +86 21 3313 8338  
Email: puneetkukreja@deloitte.com.cn



**Zhang, Boris Zhen**  
Eastern Region  
Tel: +86 21 6141 1505  
Email: zhzhzhang@deloitte.com.cn



**He, Vivi Wei**  
Southern Region  
Tel: +86 755 3353 8697  
Email: vhe@deloitte.com.cn



**Ma, Luke Kwok Kwan**  
Southern Region, Hong Kong  
Tel: +852 2852 1086  
Email: lukema@deloitte.com.hk

For more information contact visit [Deloitte.com/covid](https://www.deloitte.com/covid) or [Deloitte.com/cyber](https://www.deloitte.com/cyber)

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](https://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at [www.deloitte.com](https://www.deloitte.com).

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Deloitte brand entered the China market in 1917 with the opening of an office in Shanghai. Today, Deloitte China delivers a comprehensive range of audit & assurance, consulting, financial advisory, risk advisory and tax services to local, multinational and growth enterprise clients in China. Deloitte China has also made—and continues to make—substantial contributions to the development of China's accounting standards, taxation system and professional expertise. Deloitte China is a locally incorporated professional services organization, owned by its partners in China. To learn more about how Deloitte makes an Impact that Matters in China, please connect with our social media platforms at [www2.deloitte.com/cn/en/social-media](https://www2.deloitte.com/cn/en/social-media).

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.