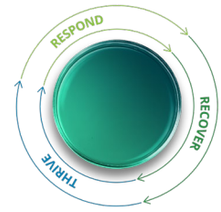
Deloitte.

Issue 6| May 13, 2020

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 involuntary 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.

Information Theft/ Leakage
Use of insider access to steal, exploit or release information

Physical Security Threats
Use of insider access to steal material items or to violate security policies

Espionage
Use of insider access to obtain sensitive info for exploitation that impacts national or corporate security and public safety

Terrorism
Use of insider access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes

Conduct Risk
Behavior that is perceived to have detrimental impacts on customers, or that could harm market integrity (e.g. violation of code of conduct)

Vendor/Supplier Risk
Captures the risks involved with entering into contracts with outside entities

Bribery/Corruption
An insider receiving money, goods or other forms of compensation to alter their behavior to benefit the giver

Security Compromise
Use of insider access to facilitate and override security countermeasures (e.g. privilege escalation, malware attack, etc.)

Insider Trading
Use of insider access to trade on insider information or influence market rates

Workplace Violence
Use of violence or threats of violence to influence others and impact the health and safety of the organization's workforce

Sabotage
Intentional destruction of equipment or IT to direct specific harm (e.g., inserting malicious code, shutting down services, etc.)

Policy Violations
Captures the risk of insiders violating organizations security and acceptable use policies

Collusion
A secret cooperation or deceitful agreement with other internal or external parties in order commit fraud or harm the organization

Coercion
The practice of persuading someone to do something by using force or threats

Other
Captures the evolving threat landscape including emerging threats not covered in the previous examples

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*

Recover and Thrive | COVID-19 spurs the next normal of insider threat management

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.

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.

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.

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.

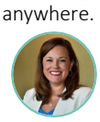
We're by your side to help you respond, recover and thrive in the wake of COVID-19

JOIN US FOR A LIVE WEBCAST:

Join us on **Wednesday, May 20 at 11:30 a.m. EDT** for a live webcast with Laurie Pezzente, Senior Vice President and Chief Security Officer of the Royal Bank of Canada, who will share her strategies to protect critical assets, customers, and people during the pandemic. This conversation will be facilitated by Emily Mossburg, Global Cyber Leader at Deloitte. We will aim to provide tangible insights to help our industries respond, recover, and thrive.

Register for the webcast

Deloitte Cyber drives progress in a dynamic, connected world, solving complex problems to build confident futures. Using human insight, technological innovation, and comprehensive cyber solutions, we manage cyber everywhere, so society – and your organization – can thrive anywhere.



Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com

Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca

Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk

Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com

James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au

Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@Deloitte.de

Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber