Guidepost

NOT SO REMOTE INSIDER THREATS

Insider threats, a security risk that comes from inside the organization itself, continue to be a risk for organizations even in the midst of a global pandemic. With many employees working remotely and dealing with the challenges COVID-19 presents, it is easier than ever for employees to be recruited even unintentionally by threat actors. That's because adversaries now have access to free or commercially available technological tools. These tools, which include forms of social media, encrypted communication platforms, and dedicated tech devices, facilitate identifying, vetting, soliciting, and staying in contact with insiders.

Social Media Has Changed the Game

Today, approximately 70% of Americans use social media to connect with one another, engage with news content, and share information. Social media has consequently become an ideal way to identify insiders and pre-vet them for an initial approach. As COVID-19 makes meeting in person increasingly difficult for the foreseeable future, many are turning toward social media to maintain the social interactions they need to feel connected. At the same time, social media has become a breeding ground for insider targeting because it provides a way to propagate disinformation and target individuals likely to be receptive to it. Even more so, it provides a means to develop relationships with organizational insiders and socialize with them. By using social media to gain an insider's trust, employees are more likely to disregard company policies and commitments.

So how does this work? This can be done via the content shared by a wayward employee, and then strategically fed to the potential insider based on his/her political views, ideologies, view of authority or establishment, etc. One strategy, long used by adversaries, has been to provide false or misleading information about their own organization. For instance, an employee might think they are simply helping a company get a foothold into a sector dominated by big tech firms or helping a journalist or graduate student understand a complex technical problem. Instead, they may be unknowingly helping a big competitor or foreign government.

Financial Pressures & Insider Threat

While some insiders may be motivated by patriotism, especially if working for a foreign government, many more insiders are influenced by financial benefit. Even for people who are gainfully employed, the financial pressures of the

current circumstances brought on by the pandemic are enormous. Individuals may be supporting family members who are out of work, or spouses who are forced to leave the workforce due to childcare requirements. The need to take care of elderly parents and relatives is another area of financial strain for individuals. Individuals with a perceived non-shareable financial problem can often present a higher risk for organizations, not just from outsiders seeking information, but also from theft (of money, assets, time) and fraudulent activity.

The Ideal Insider

Thanks to COVID-19, one element making the management of insider threats a greater challenge for businesses is the limited supervision of employees, along with the leveraging of personal devices and remote working infrastructure. The ideal mark for an insider threat is someone who is active on social media, has sufficient access to sensitive information, lacks supervision in their day-to-day work, and works remotely. Through the process of grooming, insiders can learn how to rationalize their actions through a capable adversary. The COVID-19 environment also makes the likelihood of identifying insiders much more challenging for organizations. Because of the nature of the pandemic, people do not have face-to-face interactions (in-person) and are often given more flexibility than they would have if they had to work inside an office building. In addition, the organization may be more focused on the pandemic and its financial viability than on information asset protection. This creates a prime opportunity for insider threats.

Opening Communication & Supporting Employees

While insider threats have always existed, we've established that the ground is more fertile than ever. Therefore, as an organization, it's important to reach out to employees regularly and assure them that they are not alone in dealing with the impacts of COVID-19, both personally and professionally. Frequently talk with staff to understand their level of stress and to offer them Employee Assistance Program (EAP) recourses, if necessary. Allowing employees to talk openly about their concerns and stress level is crucial to helping them navigate the pandemic. Organizations must maintain their team culture even during difficult times.

The pandemic has created a serious security risk environment for companies in which employees who would not normally engage in insider threats become more vulnerable to them. Through new technologies and new financial hardships, those looking to do harm against an organization are out there, searching for opportunities to strike. It's up to each and every company to remain vigilant and support their employees, to ensure they do not become the next insider threat target.

What Can Organizations Do?

Now that we have presented the challenges, how can organizations protect their operations in this complex environment? Here are some suggestions.

- **Conduct a Risk Assessment** to determine the level of risk the organization faces to this type of Insider Threat issue. This involves identifying critical assets (both tangible and intangible), determining likely competitors or

threat actors interested in those assets, identifying people with access to those critical assets, and establishing the organization's risk appetite.

- **Develop a Communications Initiative** to make employees aware of insider threat issues and convey the organization's approach to combating these issues for the benefit of the organization and all employees. Be sure to include information for a confidential tip line to provide employees with a means to report concerns via email, phone, or online portal.
- **Develop or Outsource Virtual Training** to educate staff about insider threat indicators and provide instructions for how to report concerns. Require employees to complete the training and deliver refresher training and updates throughout the year. Training on this matter is not a one-and-done situation. It needs to be reiterated continually.
- **Establish an Organizational-wide Check-in Process** for managers and their direct reports to enable a means for employees to share concerns and for managers to identify challenges or opportunities to assist employees with working better in the virtual environment.
- **Conduct Background Investigations** upon hiring and engage in rolling background checks for employees with critical access to information or assets. Consult with federal, state, and local requirements on this element. One of the best ways to mitigate Insider Threat is to conduct background investigations prior to hiring employees. In addition, rolling background checks play a critical role in identifying indicators of insider threats early.
- **Make EAP available for employees and encourage them to use it.** While many organizations have an EAP, many do not effectively promote it to staff. Today, we are seeing more people willing to reach out for assistance on mental health and general life challenges. This is a good development, but people need to understand how to access their EAP and be assured that contacting the EAP will not have a negative impact on their career or growth potential. Providing venues for employees to share their concerns and talk with trained staff can greatly help organizations navigate insider threats and general remote working challenges.

It is important that we recognize that this is a highly stressful time for many employees. The more that organizations can do to be transparent, reach out to employees (particularly struggling employees), vet employees via initial hiring and rolling background investigations, and offer support and resources, the greater the mitigation for insider threat issues.