UNIVERSITY OF CAMBRIDGE

Cambridge Cybercrime Centre
COVID Briefing Paper # 12

The Insider Threat Pandemic

Maria Bada **22 September 2020**

Executive summary

CCC COVID Briefing Papers are an ongoing series of short-form, open access reports aimed at academics, policymakers, and practitioners, which aim to provide an accessible summary of our ongoing research into the effects which the coronavirus pandemic (and government responses) are having on cybercrime.

In this report, we discuss how the 'insider threat' is changing in the COVID-19 pandemic, in particular, the emergence of novel factors that increase the risk of cyber-attacks and data breaches.

The new normal

It is unquestionable that the COVID-19 pandemic has led to a 'new normal' for the workforce globally. Regardless of the sector or size of an organisation, office-based employees have been asked to work remotely for extended periods. Some organisations have had to loosen controls over workforce IT systems to keep functioning and others have had to make employees redundant as a way to survive. These changes have exacerbated risks from insider threats, not only because remote-working employees are connecting from outside the organisation's network but also because those (increasingly precarious) employees may be more prone to act against the company's interests, either accidentally or intentionally.

A recent report from Deloitte [2] found that 92% of insider threat cases were preceded by a negative work event, such as a termination, demotion, or dispute with a supervisor, while 59% of employees who leave an organization (voluntarily or involuntarily) report taking sensitive data with them. The Ponemon Institutes's 2020 survey [4] calculates that the average cost of an insider threat incident has risen to $755 760, with the bulk of that money being spent on containment, remediation, incident response, and investigation.

Factors leading to an insider threat

An individual's ability to adapt to a new situation or handle stress in a normal manner is generally reduced during a crisis, especially where this relates to a prolonged series of stressful events or 'stressors' at work or home. Difficulty in handling stress can lead to panic and then to carelessness. The extended period of time that the workforce has been under stress from the pandemic has likely raised the risk from insiders. Accessing sensitive data from personal equipment or unsecured networks, along with inadequate training, can also lead to someone becoming an unintentional threat to their work environment.

In addition to unintentional lapses, we have witnessed cases during the pandemic in which employees have intentionally become an insider threat. Losing a job can lead to stress or panic while social isolation can lead people losing the sense of belonging (a lack of organisational culture). In addition, social isolation may undermine efforts at regulating behaviour; employees may be feeling more powerful and free to act from the safety of their home, without being controlled.

An example of an insider threat case during the pandemic is that of an employee of a medical device packaging company who was fired at the end of March 2020 [6]. As revenge, the employee purposely delayed and disrupted PPE shipments (with an obvious impact on the health of others) by hacking into the company's computer network through a fake user account which he created before he left the company.

In July 2020 three young hackers were charged with the hijacking of dozens of high-profile Twitter accounts [5]. Their fake tweets briefly promoted a Bitcoin scam, raking in over $100 000. The attackers posed as Twitter's remote support personnel and persuaded employees to visit a fake virtual private network page where their login information was stolen. This attack on Twitter (and several other organisations) was made easier because Twitter staff were working remotely during the COVID-19 pandemic.

The threat from employee negligence or ignorance of security threats can be exacerbated as people merge their working and home lives. Otherwise-reliable workers can expose the company to external risks due to negligence, carelessness or poor training [1]. The workload of a potential insider threat actor also directly impacts their mindset. A low workload may result in boredom or demotivation whilst a high workload may result in stress and frustration. In the context of the pandemic, both low workloads and high workloads posed by the shift to home working are likely to surface these issues, and require different approaches to solve.

Employee mindset is also affected by perceptions of the enterprise itself. A weak affiliation can cause the employee to fail to care about protecting the enterprise, whilst a strong affiliation may mean that a denial of a request made by the employee, such as a promotion, is taken much more personally, leading to thoughts of revenge [3]. Employees often feel a sense of entitlement and ownership for systems or applications that they develop from scratch. Others have a history of personal and social frustrations with the organisation, or a general lack of empathy may lead to them disregarding the impact of their actions. These reasons may cause employees to take sensitive data with them as they leave or even to sell that data to competitors. At the same time, loneliness, social naivety and the need to impress others may make them vulnerable to exploitation and manipulation from attackers who want to gain access to an organisation's assets.

Conclusions

We have briefly set out how the COVID-19 pandemic has led to an exacerbation of many factors with well-established links to unintentional or malicious insider threats. Although the PPE example showed malicious intent, the majority of insider threat cases, such as the misled Twitter employees, remain unintentional and appropriate training can reduce these, if not eliminate them altogether. However, behavioural change is always a long-term process, so it is vital that we do not delay in considering how policies and people must adjust to fit with what is going to be the 'new normal' for some time to come.

References

[1] L Coles-Kemp and M Theoharidou. "Insider Threat and Information Security Management. In: Probst C., Hunker J., Gollmann D., Bishop M. (eds) Insider Threats in Cyber Security". In: *Advances in Information Security* 49 (2010).

[2] Deloitte. *The rise of insider threats amid COVID-19*. 2020. URL: https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-cyber-COVID-19-executive-briefing-Iissue-6-release-date-5.13.2020.pdf.

[3] P Legg et al. "Towards a conceptual model and reasoning structure for insider threat detection". In: *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 4.4 (2013), pp. 20–37.

[4] Ponemon Institute. *2020 Cost of Insider Threats Report*. 2020. URL: https://www.proofpoint.com/uk/resources/threat-reports/2020-cost-of-insider-threats.

[5] RAND. *Insider Threat at Twitter Is a Risk to Everyone*. 2020. URL: https://www.rand.org/blog/2020/08/insider-threat-at-twitter-is-a-risk-to-everyone.html.

[6] Secureworld. *Insider Threat: Fired Employee Hacks to Disrupt COVID-19 Shipments*. 2020. URL: https://www.secureworldexpo.com/industry-news/insider-threat-case-delays-critical-shipments.

At the Cambridge Cybercrime Centre we make our research data available to other academics, sometimes before we have looked at it ourselves! Researchers can be provided access to our 'CrimeBB' dataset of (26 and counting) underground cybercrime forums, our extensive collections of chat channel data, and our new collections of forums relating to online right-wing extremism and radicalisation. We can also share email spam and sensor data related to DDoS and IoT malware. All these collections are regularly updated and can be rapidly provided under licence – for full details see: https://cambridgecybercrime.uk

The full set of CCC COVID Briefing Papers can be found at: https://cambridgecybercrime.uk/COVID