Insider Betrayal and Ransomware The Angelo Martino Case

Introduction

Ransomware is one of the most problematic forms of cybersecurity threats faced by businesses today. The issues are complex and have serious, far reaching repercussions. But a new case shows that things can be even worse. In 2023, a ransomware negotiator was caught working with a BlackCat ransomware gang against the very customers paying for his help to negotiate a ransom with the attackers. Angelo Martino, a 41 year old Florida resident, was accused of secretly working with the BlackCat attackers by sharing information about his customers negotiating positions and the amount of insurance coverage they had. (Lakshmanan, 2026)

Analysis

The case of Martino is also interesting from a sociological perspective. Instead of blaming Martino for his actions, one could say that he exposes a serious breach of trust in institutions and the expectation that people will generally behave professionally and honestly in their work. However, Martino and others like him are engaged in occupational deviance, using their positions to achieve illegal gains that are beneficial only to themselves. Martino is accused of having profited from the BlackCat ransomware, which he is said to have distributed to the victims of several cyberattacks in the U.S. and other countries. Through his actions, Martino clearly shows how people engage in morally questionable behavior by downplaying the potential harm they are causing through moral disengagement. There is also evidence that Martino collaborated with two other incident responders, who together attacked U.S. victims from April 2023 to November 2023 (U.S. Department of Justice, 2026). His actions, and those of others like him, reflect diffusion of responsibility.

Solutions

Stopping an insider threat is, in many ways, a social problem as much as it is a technical problem. Addressing the insider threat starts with the adoption of behavior analytics and Privileged Access Management in order to monitor employee actions for danger signs and to control access to data for those who have no business getting at it. Effective ethics training programs and strong whistleblower protections can prevent insiders from becoming threats in the first place. Fair but rigorous pre hire screening processes will be important to ensure that the right employees are hired for positions where they will be granted the level of access to data that trusted employees have. The biggest hurdle may well be the reality that organizations are hesitant to monitor their employees, in part out of fear of what may be uncovered about certain employees and also due to a general cultural aversion in the business world to doing anything that feels like spying. In many industries, monitoring employees is nothing out of the ordinary because lawyers and accountants are regularly monitored. Industry will need to develop common expectations around employee monitoring that are written in business policy.

Reflection

In this case study, we see that cybersecurity is not only about technology, it is also about people, behavior, ethics and social trust. A multidisciplinary lens from fields such as criminology, psychology and sociology is required to understand vulnerabilities that no technical solution can address.

Conclusion

The Martino case demonstrates that insider threats within the cybersecurity profession itself pose serious risks. Combating them requires not only stronger technical controls but a social science framework to understand motivation, detect deviance, and rebuild institutional trust.

References

Lakshmanan, R. (2026, April 21). Ransomware negotiator pleads guilty to aiding BlackCat attacks in 2023. The Hacker News. https://thehackernews.com/2026/04/ransomware-negotiator-pleads-guilty-to.html

U.S. Department of Justice. (2026, April 21). Florida man working as ransomware negotiator pleads guilty to conspiracy to deploy ransomware and obstruction. https://www.justice.gov/opa/pr/florida-man-working-ransomware-negotiator-pleads-guilty-conspiracy-deploy-ransomware-and