Insider Threat Mitigation: Understanding Managerial Tactics and Organizational Outcomes

Anne Kohnke, Ph.D, Associate Professor; **Tanner Flint,** BSIT Candidate;
Venkata Rathna Anirudh Mamidipaka, GRA, MSIT Candidate

College of Business and Information Technology, Lawrence Technological University

ABSTRACT

Security breaches caused by insider threats are an increasing concern as organizations are finding it more difficult to detect and prevent insider versus external cyber-attacks. While internal breaches are not as common as breaches from external actors, insider threats are still very significant. One of the main goals of external adversaries is to gain access to networks using legitimate credentials from an internal source to advance their agendas.

Whether the insiders are employees with malicious intent, do not understand or have no regard for security policies, or accidentally perform actions that put the organization at risk, insider threats can be very costly. Loss of revenue, reputation, customers, legal and regulatory requirements, are just a few areas in which organizations can be negatively impacted. The purpose of this ongoing research study is to better understand managerial tactics and organizational outcomes related to cybersecurity breaches caused by internal actors. This poster will present the findings of a literature review conducted on insider threats and discuss the research being conducted in this area.

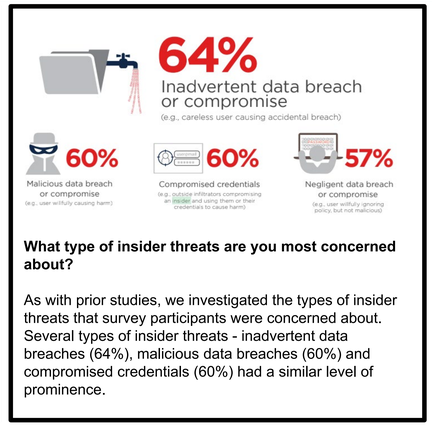
INTRODUCTION

Organizations continue to be plagued by cybersecurity breaches as noted by the numerous occurrences reported in the news. According to the Verizon 2018 Protected Health Information Data Breach Report, 58% of incidents involved insiders—healthcare is the only industry in which internal actors are the biggest threat to an organization. An insider attack is not necessarily malicious, human error (non-malicious) is a causal factor in over half of the breaches that featured an internal actor (Verizon, 2018). The consequences of insider attacks can have a significant impact on the organization in terms of loss of reputation, customers, revenue, legal liability, regulatory fines, and increased expenses for credit monitoring, to name a few. Financial gain was cited as the most frequent actor motivator for insider attacks followed by fun/curiosity, convenience, grudge, and espionage (Verizon, 2018). When it comes to patient data, unwarranted access into a patient record simply to appease curiosity is considered a breach. Admissions of family members, acquaintances, or well-known personalities into a hospital have presented temptations for employees to access that patient's medical record even though they have had no direct role in providing care or services. The quality of cybersecurity is highly related to the investments in which organization make in their cybersecurity programs (Hua & Bapna, 2013). Appropriate levels of investment in cybersecurity can enhance the capability of organizations and governments to reduce the threats from insider threat risks.

LITERATURE THEMES

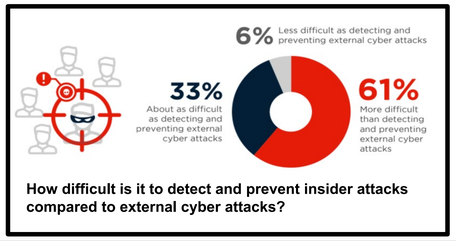
- **Malicious**
  - Inspired to antagonistically influence the organization
  - Intentional harm for personal gain
  - Typically exhibit behavior
- **Negligent**
  - Failure to understand policy
  - Overly careless
  - Complete disregard for policy
  - Failure to assign appropriate permissions
- **Accidental**
  - Unintentionally failing to follow policy
  - Falling victim to social engineering
  - Policy fails to mitigate risk of accidents

INSIDER THREATS LITERATURE REVIEW

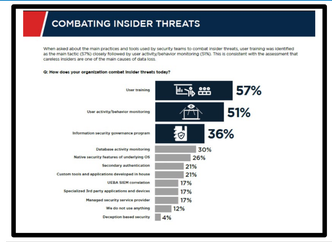


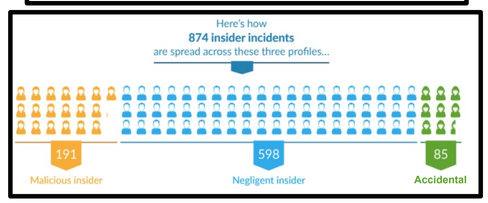
What type of insider threats are you most concerned about?

As with prior studies, we investigated the types of insider threats that survey participants were concerned about. Several types of insider threats - inadvertent data breaches (64%), malicious data breaches (60%) and compromised credentials (60%) had a similar level of prominence.



How difficult is it to detect and prevent insider attacks compared to external cyber attacks?





Only 30% of organizations feel very to extremely confident about their **insider threat security posture**. This leaves a majority of organizations in a situation that requires improved insider threat policies, training and platforms to boost insider threat confidence.

Malicious:

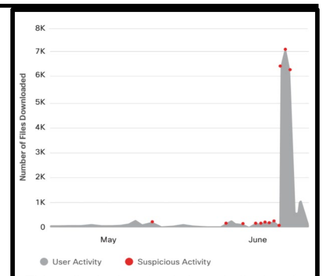
Improved Security through Information Security Governance:
Johnston and Hale (2009), determined that 50% of malicious attacks are insider abuse. They call for improved information protection programs.

Who can We Trust? The Economic Impact of Insider Threats:
Hua and Bapna (2013), ran simulations based on breach function sensitivity, deterrence level, and advantage rate for IS infrastructure and determined that investing in protection against insiders must be several magnitudes higher than for protecting against external hackers.

An Emote Opportunity Model of Computer Abuse:
Baskerville and Park (2014), developed and integrated computer abuse model that incorporates both organizational abuse settings and the psychological processes of the abuser.

Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis:
Greitzer et al. (2014), studied many insider crimes and found that the malicious offenders typically exhibited sings stress, disgruntlement, or other issues without raising alarm.

An Empirical Validation of Malicious Insider Characteristics:
Liang et al. (2016), say that malicious insiders continue to pose a great threat to organizations due to their knowledge and access to organizational resources. They can launch attacks with far more damaging impacts than outsiders.



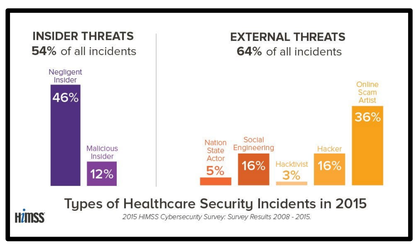
This spike in downloads is an indicator of malicious activity.

Negligent:

Information systems user security: A structured model of the knowing–doing gap:
James Cox (2002), creates a structured model that provides a framework and description of user information security behavior and the "knowing-doing gap".

Data minimisation in communication protocols: a formal analysis framework and application to identity management:
Meilof Veeningen et al. (2014), provide ways that reduce the amount of data users interact with.
This prevents insiders from having the option to disregard policy and access information that they shouldn't.

Insider threat mitigation: preventing unauthorized knowledge acquisition:
Qussai Yaseen and Brajendra Panda (2012), investigated the insider threat in relational database systems. They provide theorems and proofs to support proposed solutions that prevent the insider threat without limiting the availability of data.

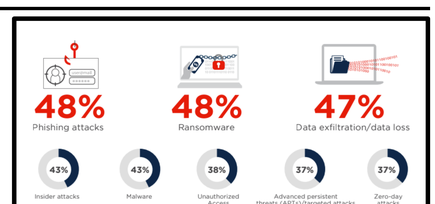


Accidental:

Enemy at the Gate: Threats to Information Security:
Whitman (2003), discusses the act of human failure. Employees may accidentally activate a virus or worm that could be detrimental to the organization.

An Adaptive Risk Management and Access Control Framework to Mitigate Insider Threats:
Baracaldo and Joshi (2013), develop a framework that helps organizations determine appropriate permissions for users in an effort to reduce loss when credentials are compromised.

Risk perceptions of cyber-security and precautionary behavior:
Schaik et al. (2017), discuss the perceived risk of various hazards in cybersecurity. Social engineering, keyloggers, viruses and worms are all major concerns in cybersecurity. These are issues associated with accidental insider threat.



Which cyberthreats are you most concerned about?

REFERENCES

Baskerville, R., Park, E., & Kim, J. (2014). An emote opportunity model of computer abuse. *Information Technology & People*, 27(2), 155-181. doi:10.1108/ITP-11-2011-0068

Baracaldo, N., & Joshi, J. (2013). An adaptive risk management and access control framework to mitigate insider threats. *Computers & Security, 39, 237.*

Bock, O. (2017, March 02). 12 Surprising Facts You Didn't Know About Insider Threats. Retrieved March 28, 2018, from https://www.onionid.com/blog/insider-threats-12-surprising-facts-you-didnt-know- about/

Cox, J. (2012). Information systems user security: A structured model of the knowing-doing gap. *Computers in Human Behavior*, 28(5), 1849-1858. doi:10.1016/j.chb.2012.05.003

Hua, J., & Bapna, S. (2013). Who Can We Trust?: The Economic Impact of Insider Threats. *Journal of Global Information Technology Management*, 16(4), 47-67. doi:10.1080/1097198x.2013.10845648

JOHNSTON, A. C., & HALE, R. (2009). Improved Security through Information Security Governance. *Communications Of The ACM*, *52*(1), 126-129. doi:10.1145/1435417.1435446

Liang, N., Biros, D., & Luse, A. (2016). An empirical validation of malicious insider characteristics. Journal of Management Information Systems, 33(2).

Greitzer, F.L., Kangas, L.J., Noonan, C.F., Brown, C.R., & Ferryman, T. (2014). Psychosocial modeling of insider threat risk based on behavioral and word use analysis. (2013). *E-Service Journal*, 9(1), 106-138.

Schulze, H. (2017). THREAT 2017 REPORT MONITORING, DETECTION & RESPONSE (Tech.).

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75, 547-559. doi:10.1016/j.chb.2017.05.038*

Veeningen, M., Weger, B., & Zannone, N. (2014). Data minimisation in communication protocols: a formal analysis framework and application to identity management. *International Journal Of InformationSecurity*, 13(6), 529-569. doi:10.1007/s10207-014-0235-z

Verizon. (2018). *Verizon 2018 Protected Health Information Data Breach Report.* Verizon.

Whitman, M. (2003). Enemy at the gate : Threats to information security. *Communications of the ACM, Vol. 46 No. 8 (ago. 2003), P91-95.*

Yaseen, Q., & Panda, B. (2012). Insider threat mitigation: Preventing unauthorized knowledge acquisition. *International Journal of Information Security*, 11(4), 269-280. doi:10.1007/s10207-012-0165-6