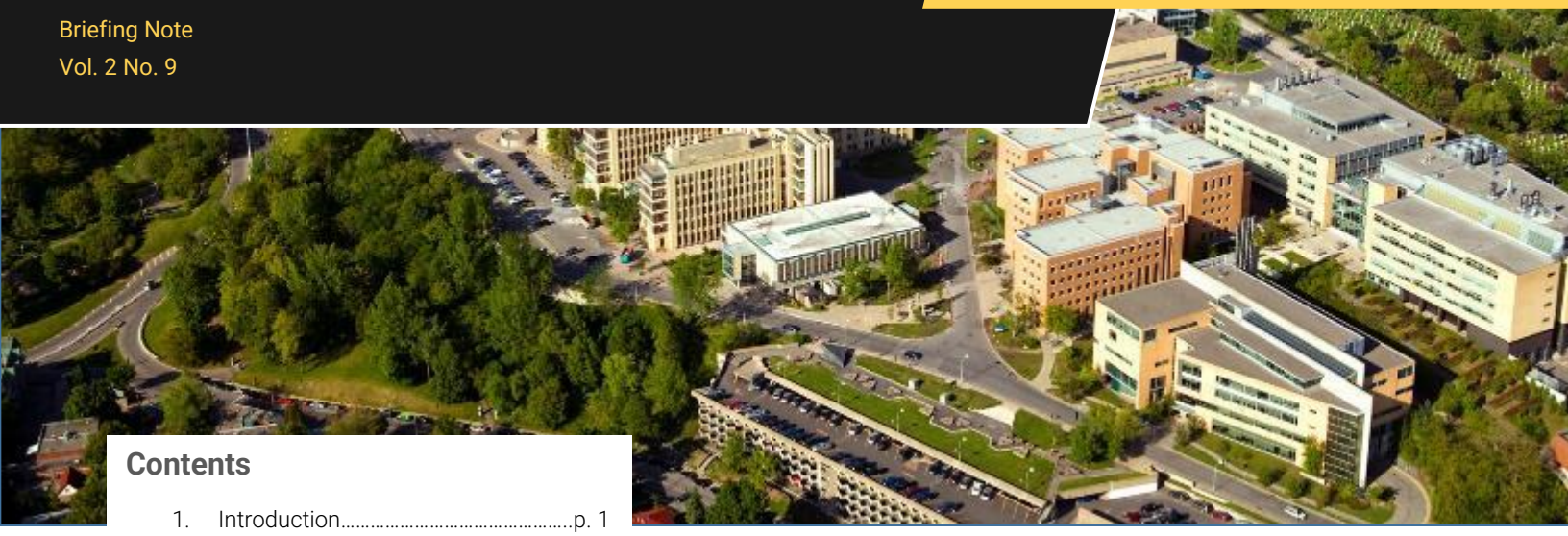
Intrusion Detection Systems

Traian Toma, Master's Candidate

RCCP | Research Chair in Cybercrime Prevention

Briefing Note
Vol. 2 No. 9



Contents

Introduction

Organizations need to remember that cyber threats may already be lurking within.[1] Studies on detecting and predicting insider threat increased after media coverage of the Snowden case in 2013.[2] Procedures for monitoring computer systems and networks—deployed by almost half of Canadian businesses[3]—have also been adapted to identify employees with malicious intent.[4]

Intrusion detection systems (IDSs) are tools that scan computer systems or networks to identify security policy violations and report them to cybersecurity analysts.[5]

Organizations install IDSs to deter malicious employees but implementing these tools can exacerbate insider threat if potential negative reactions are not considered.

The Research Chair in Cybercrime Prevention was created on the initiative of Université de Montréal, Desjardins and the National Bank of Canada. Headed by Benoît Dupont, a researcher at the International Centre for Comparative Criminology at Université de Montréal, its mission is to contribute to the advancement of research into cybercrime phenomena with a view to prevention.

An overview of IDSs

There are 2 types of IDSs, each using different data:

Network IDSs scan the network at any given time, analyzing information that is typically encapsulated in packets.[6]

These packets contain, among other things, the inbound and outbound IP addresses related to the information in question.

- Host-based IDSs collect data from individual computers (system calls, keystroke or mouse dynamics, logging, registry, etc.).

The majority of scientific studies recommend host-based IDSs to combat insider threat, as malicious employees are already on the company network and can, for example, use the IT systems to gain unauthorized access to confidential files and copy them to removable media.[6, 7, 8, 9] Despite their popularity, **host-based IDSs are insufficient,** as more than half of data exfiltration cases are carried out over networks. Insiders primarily use their business email address to send confidential company data to a recipient outside the network.[9]

IDSs also use two main techniques to detect an intrusion. **Signature-based detection** uses pattern-matching techniques (hence the notion of "signatures") to detect threats.[10] IDSs based on this technique are easy to implement as they merely compare the data to the signature database.[11] For example, an IDS can detect exfiltration of confidential data by flagging instances where someone is sending attachments that exceed a threshold size predetermined by the developers.[12] These indicators aren't immune to false positives; an employee could very well legitimately send a large number of files externally. In addition, signature based IDSs only identify known threats, and the signature database must be updated constantly for them to be effective.[11, 13]

This detection technique is particularly ineffective against zero-day vulnerabilities, or those unknown to everyone but the attackers.[14]

Anomaly-based detection involves training the IDS to recognize typical activities within any system or network. It can then report any unusual IT events. For example, researchers[15] have developed an algorithm that assesses and detects anomalies based on the user's normal logon frequency, the number of emails sent and received, and the destination and origin of the emails in question.

Organizations are more likely to opt for anomaly-based detection, as it helps identify previously unknown attacks.[2] However, it's likely to produce false positives, particularly in dynamic workplaces where behaviours within the IT system or network vary according to the requirements of various business projects.[16] Employee rotation in the workplace can also trigger changes in the organization's normal activities.[6] Moreover, the algorithm may mistake malicious operations for typical activities during the IDS's learning phase.[11] Developers must reset the process or install a dynamic algorithm that adjusts to changes in IT events[6]

The majority of IT activities are benign,[17] which explains why some studies have attempted to incorporate additional behavioural and psychological indicators into IDSs to reduce the rate of false positives.[6] This approach suggests that malicious insiders have certain distinct personal characteristics, which would enable cybersecurity analysts to conduct an initial screening of IDS alerts, focusing on at-risk individuals.[18, 19] One team of researchers has developed an algorithm to predict the level of risk posed by an employee using 12 psychosocial precursors to insider threat.[20] In another study, researchers built a tool that deduces personality traits conducive to internal threat—namely narcissism, Machiavellianism and thrill seeking—from the content of websites regularly visited by the individuals studied.[19] Lastly, researchers in another study[21] developed a model for detecting anti-authority behaviours based on comments made on YouTube concerning law enforcement, contending that this trait is associated with insider threat.

Other IDSs use human resource data,[6, 12] such as employee user accounts expiring within 30 days, as it's been posited that most insider threat incidents involved employees who received a notice of termination and that the attacks occurred between receiving the notice and the employment end date. It's important to note that psychosocial data is used to supplement IDSs and facilitate risk management; this data alone cannot indicate the presence of a malicious insider,[22] especially since insider threat represents a very

small part of an organization's work force[23] (for more information on the psychosocial factors of insider threat, see Briefing Note Vol. 2 No. 8).

The deterrent effect of IDSs

IDSs are based on the principle of threat deterrence. Organizations hope to increase the certainty of IDS detection and thus deter security policy violations.[5] There are no studies on the deterrent effect of IDSs, but those on digital monitoring technologies (tracking internet use, recording network activities, security audits, etc.) contain relevant details that could be applied to IDS. One study[24] found that digital monitoring increases employee perceptions of certainty and severity of penalty. Other studies show that perceived certainty of penalty leads to compliance with security rules, as well.[25,26] However, according to the first study mentioned above, perceived certainty of penalty mainly affects employees who share the organization's values, as they're more mindful of the organization's reputation.[24] In addition, surveillance technologies heighten perceived severity of penalty, as they make it easier to detect violations that result in severe disciplinary action (such as dismissal). According to another study, digital surveillance on its own appears to have a greater deterrent effect than organizational cybersecurity policies.[25]

The adverse effect of surveillance technologies

While IDS detection capabilities appear at first glance to have a certain deterrent effect on insider threat, strictly one-way implementation may result in unintended consequences and exacerbate insider threat within an organization. In other words, deterrence fails to consider the moral values of employees and how they may conflict with perceptions of certainty and severity of penalty. Perceptions of severity of penalty erode the climate of trust within the workplace and subsequently exacerbate non-compliance, even among those who had previously identified with the company's values.[27] Some authors argue that digital monitoring reduces organizational commitment among employees.[28] More specifically, altruistic actions that go beyond an employee's formal obligations within the organization decrease in response to surveillance.[29, 30] One study demonstrated that electronic surveillance reduces workers' perception of their relationship with their employer to a strictly economic and utilitarian one; these employees will perform their formal duties in exchange for remuneration, but they won't be incentivized to take initiative or to innovate in favour of the organization.[30]

Psychological reactance theory presupposes that each person possesses a certain level of individual freedom their daily life, the threat to which engenders reactance.[31] Reactance is a negative emotional response that motivates resistance to the threat in question (in this case surveillance technologies) in order to preserve the sense of individual freedom. For example, deviance in the workplace increases when companies that promote employee autonomy simultaneously introduce surveillance measures, [33] as workers become uncertain about the level of control they have over their work. Surveillance measures infringe on the sense of freedom, driving employees to rebel in order to regain a certain autonomy. The implementation of IDSs to ensure compliance with rules may therefore frustrate employees who wish to carry out their duties on their own initiative and elicit reactance.

Some researchers have demonstrated that giving a perception of autonomy eliminates negative attitudes toward electronic surveillance—such as feelings of invasion of privacy or the sense that an organization mistrusts its employees—that are conducive to deviance in the workplace.[34] According to this study, giving employees a sense of control helps mitigate their reactance, thus preventing autonomy from conflicting with surveillance.[33] The differing conclusions of these

studies may be attributed to differences in the samples studied (student population[33] versus company employees[34]).

Another issue related to surveillance technologies is privacy. According to communication privacy management theory, individuals believe they have a right to privacy, regardless of the legal context.[35] They set boundaries around the information they choose to disclose and renegotiate them depending on the context. Therefore, employees generally expect to partially concede to incursions into these boundaries for the purpose of surveillance.[35] However, complications can arise when organizations violate boundaries that were initially negotiated in a more or less explicit way.[35, 36] This creates a climate of mistrust.[36] For example, collecting information not related to the job may cause tension.[37]

Research shows that employees who are predisposed to reactance have a greater perception of electronic surveillance as an invasion of their privacy and are thus more likely to disobey organizational cybersecurity policies as a means to regain their freedom.[38] Ethical orientation is another element moderating workers' reaction to surveillance technologies.[39] Individuals predisposed to utilitarianism tolerate their use despite privacy breaches if they believe they're essential to the proper management of the organization. There's also little concern among formalists, that is, those who believe that obedience to rules goes hand in hand with moral conduct.

Limitations and recommendations

IDSs are an innovative way to detect insider threat, but studies of their effectiveness are inconclusive. In most cases, the IDS studied was only able to be tested once, as the authors failed to provide details on the algorithm's construction process and performance.[2] Furthermore, experiments use simulated attacks, as access to real databases is difficult to obtain.[14]

It's therefore important for practitioners to recognize that the outcomes may be different on the ground.

In addition, some studies focusing more specifically on psychosocial data may provide an inaccurate portrayal of insider threat due to the operationalization of risk factors. For example, contempt for authority is undeniably a risk factor for insider threat,[20] but measuring it from messages about law enforcement on social media[21] becomes problematic if the broader social context is ignored. Furthermore, the studies in question don't sufficiently address the potential unintended negative consequences of reactance and the subsequent resistance to security policies.

A better understanding of the human factors of insider threat can better equip organizations to deal with this type of issue. Recommended actions include:

- Using feedback mechanisms, considering employees' feelings about the information captured by IDSs. Research indicates that this promotes a sense of consultation and agency in the design of organizational procedures[29] and decreases perceptions of privacy invasion when psychosocial data is examined.[37, 40] It also avoids an imbalance between the actions of the organization and the expectations of employees.[35]

- Giving employees more autonomy in how they perform their daily tasks. This increases their sense of control and will mitigate the negative effects of surveillance technologies.[34]

- Explaining the implementation of electronic surveillance, taking care to design the message in a way that incorporates employees' ethical orientations.[39] For example, managers should emphasize the importance of IDSs in maintaining smooth operations to appease utilitarians.

In sum, organizations implementing IDSs must be careful not to sacrifice workplace solidarity and

commitment in their efforts to prevent insider threat. The values that employees embrace and that influence their compliance with rules, their productivity and their sense of innovation outweigh the effects of deterrence.

References

[1] Bellovin, S. M. (2008). The insider attack problem: nature and scope. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith and S. Sinclair (ed.), *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 5–16). Boston, MA: Springer US.

[2] Gheyas, I. A. and Abdallah, A. E. (2016). Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Analytics, *1*(1), 1–29.

[3] Statistics Canada. (2018). Statistics Canada - SERENE-RISC. https://www.serene-risc.ca/en/statistics-canada

[4] Liu, A., Martin, C., Hetherington, T. and Matzner, S. (2005). A comparison of system call feature representations for insider threat detection. Paper presented at the Sixth Annual IEEE SMC Information Assurance Workshop (pp. 340–347).

[5] Scarfone, K. and Mell, P. (2012). Guide to Intrusion Detection and Prevention Systems (IDPS) (Draft) (pp. 1–111). ÉU: National Institute of Standards and Technology.

[6] Liu, L., De Vel, O., Han, Q.-L., Zhang, J. and Xiang, Y. (2018). Detecting and preventing cyber insider threats: A survey. IEEE Communications Surveys Tutorials, *20*(2), 1397–1417.

[7] Kozushko, H. (2003). Intrusion detection: host-based and network-based intrusion detection systems, 1–23.

[8] Han, K., Mun, H., Yeun, C. Y. and Kim, K. (n.d.). Design of intrusion detection system preventing insider attack, 419–430.

[9] Cappelli, D., Moore, A. and Trzeciak, R. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (theft, sabotage, fraud). Addison-Wesley.

[10] Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, *2*(1), 1–22.

[11] Rao, U. H. and Nayak, U. (2014). Intrusion detection and prevention systems. In U. H. Rao and U. Nayak (ed.), *The InfoSec Handbook: An Introduction to Information Security* (p. 225–243). Berkeley, CA: Apress.

[12] Hanley, M. and Montelibano, J. (2011). Insider threat control: using centralized logging to detect data exfiltration near insider termination, 1–23.

[13] Penta Security. (2016). The benefits of using signature-less detection technology. Penta Security Systems Inc.

[14] Azeez, N. A., Bada, T. M., Misra, S., Adewumi, A., Van der Vyver, C. and Ahuja, R. (2020). Intrusion detection and prevention systems: an updated review. N. Sharma, A. Chakrabarti and V. E. Balas (ed.), Paper presented at Data Management, Analytics and Innovation, Singapore (pp. 685–696).

[15] Kim, J., Park, M., Kim, H., Cho, S. and Kang, P. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences*, *9*(19), 1–23.

[16] Chae, Y., Katenka, N. and DiPippo, L. (2019). An adaptive threshold method for anomaly-based intrusion detection systems. 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA) (pp. 1–4). 10.1109/NCA.2019.8935045

[17] Azaria, A., Richardson, A., Kraus, S. and Subrahmanian, V. S. (2014). Behavioral analysis of insider threat: a survey and bootstrapped prediction in imbalanced data. *IEEE Transactions on Computational Social Systems*, *1*(2), 135–155.

[18] Liang, N. (Peter), Biros, D. P. and Luse, A. (2016). An empirical validation of malicious insider characteristics. *Journal of Management Information Systems*, *33*(2), 361–392.

[19] Alahmadi, B. A., Legg, P. A. and Nurse, J. R. C. (2015). Using Internet activity profiling for insider-threat detection.

[20] Greitzer, F. L., Kangas, L. J., Noonan, C. F., Dalton, A. C. and Hohimer, R. E. (2012). Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. Paper presented at the 45th Hawaii International Conference on System Sciences (p. 2392–2401).

[21] Kandias, M., Stavrou, V., Bozovic, N. and Gritzalis, D. (2013). Proactive insider threat detection through social media: the YouTube case. Paper presented at the 12th Workshop on Privacy in The Electronic Society, Berlin, Germany (pp. 261–266). 10.1145/2517840.2517865

[22] Legg, P. A., Moffat, N., Nurse, J. R. C., Happa, J., Agrafiotis, I., Goldsmith, M. and Creese, S. (2013). Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *4*(4), 20–37.

[23] Pfleeger, C. P. (2008). Reflections on the insider threat. In S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith and S. Sinclair (ed.), *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 5–16). Boston, MA: Springer US.

[24] D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79–98.

[25] Herath, T. and Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165.

[26] Kuo, K.-M., Talley, P. C. and Cheng, T.-J. (2019). Deterrence approach on the compliance with electronic medical records privacy policy: the moderating role of computer monitoring. *BMC Medical Informatics and Decision Making*, *19*(1), 1–12.

[27] Li, H., Zhang, J. and Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4), 635–645.

[28] Tabak, F. and Smith, W. P. (2005). Privacy and electronic monitoring in the workplace: a model of managerial cognition and relational trust development. *Employee Responsibilities and Rights Journal*, *17*(3), 173–189.

[29] Jahangir, N., Akbar, M. M. and Haq, M. (2004). Organizational citizenship behavior: Its nature and antecedents. *BRAC University Journal*, *1*(2), 75–85.

[30] Jiang, H., Siponen, M. and Tsohou, A. (2019). A field experiment for understanding the unintended impact of internet monitoring on employees: policy satisfaction, organizational citizenship behaviour and work motivation.

[31] Lowry, P. B. and Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, [25](5), 433–463.

[32] Lawrence, T. B. and Robinson, S. L. (2007). Ain't misbehavin: Workplace deviance as organizational resistance. *Journal of Management*, *33*(3),

[33] Jensen, J. M. and Raver, J. L. (2012). When self-management and surveillance collide: Consequences for employees' organizational citizenship and counterproductive work behaviors. *Group & Organization Management*, *37*(3), 308–346. 10.1177/1059601112445804

[34] Martin, A. J., Wellen, J. M. and Grimmer, M. R. (2016). An eye on your work: How empowerment affects the relationship between electronic surveillance and counterproductive work behaviours. *The International Journal of Human Resource Management*, *27*(21), 2635–2651.

[35] Watkins A., M., Coopman, S. J., Hart, J. L. and Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. Management Communication Quarterly, 21(2), 172–200. 10.1177/0893318907306033

[36] Snyder, J. L. (2010). E-mail privacy in the workplace: a boundary regulation perspective. The Journal of Business Communication, 47(3), 266–294. 10.1177/0021943610369783

[37] Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797–804. 10.1037/0021-9010.86.4.79

[38] Yost, A. B., Behrend, T. S., Howardson, G., Badger Darrow, J. and Jensen, J. M. (2019). Reactance to electronic surveillance: A test of antecedents and outcomes. *Journal of Business and Psychology*, *34*(1), 71–86.

[39] Alder, G. S., Schminke, M., Noel, T. W. and Kuenzi, M. (2008). Employee reactions to internet monitoring: the moderating role of ethical orientation. *Journal of Business Ethics*, *80*(3), 481–498.

[40] Posey, C., Bennett, R., Roberts, T. and Lowry, P. (2011). When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, *7*, 24–47.