Information Security Journal: A Global Perspective

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/uiss20

A primer on insider threats in cybersecurity

Sunitha Prabhu & Nik Thompson

To cite this article: Sunitha Prabhu & Nik Thompson (2022) A primer on insider threats in cybersecurity, Information Security Journal: A Global Perspective, 31:5, 602-611, DOI: 10.1080/19393555.2021.1971802

To link to this article: https://doi.org/10.1080/19393555.2021.1971802

Published online: 07 Sep 2021.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2022, VOL. 31, NO. 5, 602–611
https://doi.org/10.1080/19393555.2021.1971802

Taylor & Francis
Taylor & Francis Group

Check for updates

A primer on insider threats in cybersecurity

Sunitha Prabhu[a] and Nik Thompson[b]

[a]School of Computing and Mathematical Sciences, University of Waikato, Hamilton, New Zealand; [b]School of Management, Curtin University, Perth, Australia

ABSTRACT
Though human factors are increasingly being acknowledged as a contributor to cybersecurity incidents, this domain is not widely understood by those in technical and applied disciplines. Humans can be influenced, are not always rational or predictable, and must be studied through psychology rather than technology. Consequently, this domain may represent uncharted territory for the technical practitioner leaving many promising areas of research and practice unexplored. This paper provides a broad primer on human factors in cybersecurity, specifically focusing on the threat posed by organizational insiders. We emphasize the pivotal role that users play in determining overall system security and aim to introduce non-experts to this field, stimulating new interest in this intersection of humans and computers.

KEYWORDS
Cybersecurity; human factors; insider threat; security breach

1. Introduction

While it is widely accepted that information security is critical for an organization’s long-term success, what is less apparent is that this security depends collectively on every individual who may have access to organizational infrastructure (Cuchta et al., 2019). Rapid changes in technology in the recent decades have also changed information security and privacy needs. All over the world, privacy laws have changed to keep up with the new developments (Privacy Act, 2020). The primary focus of information security controls is to protect the confidentiality, integrity, and availability of information systems without hindering the organization’s efficiency. Security models are historically focused on principles such as perimeter control and intrusion detection. These principles originate from simple physical security (for example, walls and fences) and have been successfully applied to the digital environment over time. In these models, human factors may be overlooked and undervalued but, in practice, play a significant role in security (Orshesky, 2003). An over-dependence on technology alone can render an organization vulnerable as unaddressed human factors, though subtle, may be highly impactful for security (Colwill, 2009). Lacombe suggests that human beings are the weakest link in cybersecurity and that attacks increasingly target people, especially those with a lack of expert knowledge. Greenberg (2015) reports that human error accounts for 52% of the root cause of security breaches. 42% of these cited end-user failures to follow procedures, 42% cited general carelessness, 31% cited failure to get up to speed on new threats, 29% cited lack of expertise with applications, and 26% cited IT staff failure to follow policies and procedures.

As humans can only be understood by psychology rather than technology, this can pose an issue for information security practitioners. Academic research on human factors draws heavily from the social sciences and behavioral psychology and can require a different skillset and background than that commonly required for information security work. This steep learning curve may hinder technical experts from delving into this promising area. We, therefore, present a primer on insider threats in cybersecurity, covering the causes, types, and effects of insider threats and elaborate the methods and motives of the insider threats in an easily

CONTACT Sunitha Prabhu sunitha.prabhu@waikato.ac.nz School of Computing and Mathematical Sciences, University of Waikato, Hamilton, New Zealand

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

accessible form. Through this, we hope to stimulate new interest in the field and emphasize its broad applicability across different industries and areas of security.

In the next section, we give a brief overview of the relevance of this work. This is followed by a literature review on insider threats to information security. In section 4, we discuss the implications and recommend future directions. Finally, we conclude our paper with the findings in section 5.

2. The role of human factors

The success or failure of any security program is dependent upon the people who design, manage, and work with the processes and technologies, such as system developers, administrators, and end-users (Orshesky, 2003). A security threat could be from anyone with access, authorized or unauthorized, to an organization's information systems (Proctor et al., 2009). A human attacker can utilize motivation, creativity, and ingenuity, making the threat complex and challenging to predict and challenging to analyze (Akhunzada et al., 2015).

To present a fuller understanding of security threats and identify those caused by human factors, we report on a review of prior work on threats caused by human factors. This includes scholarly articles as well as published reports of data breaches. The articles were analyzed to find the causes and impact of human factors on cybersecurity breaches. The findings help us understand the significant part that human factors play in security data breaches and how these factors relate to other organizational conditions.

2.1. Risk to cybersecurity

Cybersecurity is not just the act of responding to an incident but also learning from one and preparing to avoid or defend future incidents (Spring & Illari, 2019). With organizations increasingly moving to computer-based information management and the growing integration of outsourcing, off-shore work, and remote offices, security threats and risks to their systems have increased significantly (Prabhu & Thompson, 2020). Threat and risk assessment is commonly described in terms of the CIA triad of confidentiality, integrity, and availability (Jones & Colwill, 2008).

- *Confidentiality* is ensuring that information assets remain private and are not viewed by or disclosed to individuals who are not authorized to receive them (Elmrabit et al., 2015).
- *Integrity* is ensuring that information assets cannot be modified without authorization and the existing record relates to the actual history of the record (Elmrabit et al., 2015; Jones & Colwill, 2008). It is to ensure the accuracy, consistency, and trustworthiness of the data at any point in time.
- *Availability* is ensuring that information assets are only available when requested by an authorized individual, and all authorized users can have uninterrupted access (Elmrabit et al., 2015; Wall, 2013).

All three of these core domains in risk assessment can be influenced by human factors.

2.2. Causes of human threats

As sensitive data is no longer confined within an organization's premises, there are increasing opportunities for security breaches. Jones and Colwill (2008) explain that the human threat could be from outsiders, current employees, outsourced employees, or former employees that might know the information, location, and vulnerabilities that can be exploited. Prominent in prior work is the view that motive, opportunity, and capability are among the main factors for attacks (Hunker & Probst, 2011; Jones & Colwill, 2008). These factors are explained briefly below:

- *Motivation* is the core reason to carry out the attack (Ghafir et al., 2016). This is the users' internal or personal drive to access information assets for wrongful purposes (Elmrabit et al., 2015; Jones & Colwill, 2008). The motivation for a cyber-attack can be due to a feeling of revenge (Hadlington, 2018), for personal gains, technical challenge, curiosity, espionage, fun, or a combination of these factors (Hunker & Probst, 2011).
- *Opportunity* involves having access and time for the attacker to execute the attack. An opportunity for an insider can arise because of

authorization to access systems, familiarity with the location, and knowledge of the type of information (Colwill, 2009; Jones & Colwill, 2008).

- *Capability* is having the required tools, skills, and resources to execute an attack (Ghafir et al., 2016). Insiders have knowledge of information assets and loopholes, authorized access to information assets, and the ability to identify weaknesses for successful attacks (Colwill, 2009; Jones & Colwill, 2008).

Elmrabit et al. (2015) explain that while motive comes from personal drivers, opportunity and capability is overtly given by the organization to the insider to perform their role. An insider either bumps into an opportunity causing an accident or creates an opportunity by either omission (i.e. failing to perform the policy requirements) or commission (i.e. violating the computer use policy). Such actions could compromise the organization's information confidentiality, integrity, and availability.

2.3. *Sources of human threat*

Over a decade ago, it was perceived that technology was the answer to information security problems, and the role of human factors leading to security breaches was under-addressed (Colwill, 2009). Unsurprisingly, there is a shift toward understanding various human factors that affect cybersecurity (Jeong et al., 2019). A security breach can come in many forms, such as hacking, physical loss, portable device misplacement, and unintentional disclosure (Li et al.,).

Wall (2013) explains that information security is predominantly focused on preventing access to malicious outsiders such as hackers or scammers. Thus, organizations tend to be more sensitive to external threats rather than insider threats. In recent years malicious insiders have emerged in the threat landscape (Wall, 2013). While the outsider threat is indeed serious, they have limited opportunity to carry out their attacks as they must gain access by exploiting gaps or weaknesses in the system (Walton & Limited, 2006). In contrast, insiders can cause damage with relative ease as they have already have access to the information and the organization's policies, procedures, and technology (CERT, 2016). We summarize the characteristics of the insider and the outsider threat in Table 1.

Table 1. Insider-threat vs outsider-threat.

Characteristics	Insider-threat	Outsider-threat
Intentional motive	May be intentional, but could be accidental.	Always intentional.
Malicious intent	May be malicious, non-malicious, or no intent.	Mostly malicious. In rare cases it can be to show-off or demonstrate their technical skills.
Authorization	An authorized user (current or former).	Generally, an unauthorized user who gained access through wrongful means.
Access methods	Mostly direct access due to knowledge of organizational procedures.	Needs access to many sources of intelligence/ information before they can act.
Opportunity	Have a significant opportunity due to legitimate access to the system.	Limited opportunity to carry out their attacks as they must gain access by exploring gaps or weaknesses in the system.
Expertise	Does not necessarily need expertise, especially if unintentional.	Expertise is needed to gain access to hardware and software.
Security policy awareness	Will be aware or have access to organizations security policy.	Mostly will be prepared to target the 'usual' organizational policies but not specific for any organization.

Furthermore, if technical security controls are sound, an outsider attack may also trick unsuspecting insiders into opening the doors for them, for example, enticing them to click links to a site (Giandomenico & Groot, 2018). Anonymity and lack of accountability also play a significant role in facilitating an insider to act unseemly as most individuals have inhibitions of being caught (Jones & Colwill, 2008). The difficulty distinguishing an insider's activity from benign activity generates an opportunity for insiders (Hunker & Probst, 2011).

There is an ongoing debate on the risk of insider threats compared to outsider threats. The study performed by Giandomenico and Groot (2018) with 47 data security experts show that organizational awareness of insider threats is increasing. Historically, the organizational losses due to outsider breaches are better understood, as the threats from the insider are more challenging to detect and prevent. In some cases, an insider may know how to achieve the most significant impact while leaving little evidence due to their legitimate access to information, location of assets, and organization knowledge (Colwill, 2009). Both outsiders and insiders ultimately cause harm to the organization by exploiting the organization's vulnerabilities (Wall, 2013).

2.4. *Effects on the organization*

Human factors have serious implications for an organization's information security resulting in long-term reputational damages, consequently leading to financial losses (Nobles, 2019). Despite information security being crucial to the organization, breaches are usually detected months after they occur (Spring & Illari, 2019). While the exact impact of information security breaches on the organization is unknown due to the lack of effective metrics, tools, and frameworks (Agrafiotis et al., 2016), various types of harm caused have been identified by researchers.

Agrafiotis et al. (2016) categorize harm resulting from cyber-attacks as physical harm (loss of information or system unavailability), economic harm (with a negative financial consequence), psychological harm (mental well-being and psyche), reputational harm (damage to the public image of an organization), and societal harm (result in a social context). It is crucial to note that the harm types may not necessarily be distinctive and could overlap, primarily to economic harm.

Organizations currently calculate the harm as financial damages from the stock-market exchanges and ignore the resulting psychological harm on their customers and employees. When an organization is a victim of a cyber-attack, the impact is not only on the organization but also on its employees and customers. The most prominent harm to the organization is reputational damage, which may lead to a damaged relationship with customers, consequently leading to economic harm (Agrafiotis et al., 2016). A security breach, in whatever form, can result in loss of morale and trust in the organization for employees, thereby changing the relationship between the employee and the workplace (Wall, 2013). Harm resulting from loss of trust from an employee or a customer may not always be visible and may have more long-term effects.

3. Insider threats

An insider is a person who has authorized access and inside knowledge of the company (NAIC, 2008). Prabhu and Thompson (2020) define an insider as *a current or former employee, contractor, or another business partner who has or had authorized access to the organization's network, system, or data*. We use this reference definition in this study. There are some variations to how researchers define insiders. While some insider definitions include recently discharged employees whose system credentials have not yet been revoked, others include contractors and former employees in general since they might possess knowledge of the organization's policies, procedures, and information access methods (CERT, 2018; Elmrabit et al., 2015; Jones & Colwill, 2008). Even a discharged employee whose system credentials have been revoked may continue to be a threat unless the organization modifies their information access methods. CERT (2018) defines an insider threat as a threat resulting from an insider causing harm or substantially increases the probability of future harm to the confidentiality, integrity, or availability of the organization's information systems. Occasionally, employees that have changed roles may continue to maintain and use privileges of their previous authority.

In any computing environment, the human threat to information assets can come in various forms – unwilling, intentional or accidental, malicious or non-malicious, obvious or stealthy, technical or non-technical, individual or organized. This section describes the main types of insider threats to cybersecurity and explains the methods and motivations.

3.1. *Insider threat methods*

An insider threat can manifest in many ways. Chabinsky (2010) recognize insider threats to include intentional fraud, theft of intellectual property (IP), IT sabotage, or even an unintentional breach caused by a well-intentioned employee. Furthermore, organizations could be affected by more than one category of insider threats at the same time. We identify some of the methods that the human factor acts as a threat. We map these human factors threats to a high, medium, or low ranking for the motive, opportunity, and capability and summarize them in Table 2.

Any type of threat may occur in different frequencies, present different levels of risk to the organization, and be composed of a different balance of motive, opportunity, and capability. Unintentional acts have no motive or intention to harm; they are caused by accident and hence are given no ranking for the motive. The other methods of insider threats are intentional acts to harm the organization and hence are given a ranking of high for the motive. The ranking for an opportunity for unintentional methods is given to be medium, given the control mechanism relaxations and access privileges an insider may have as compared to an outsider. The authorized access granted to an insider by the organization gives them the required opportunity and capability to carry out an act of IP theft or fraud. Hence, the opportunity for these two methods is given a high ranking, and the capability is given a medium ranking as they may not always have the privileges to access all information. Acts of insider social engineering and IT sabotage will need more effort by an insider than just having the authorization to access the systems. Hence, the opportunity and capability for these two methods are given a ranking of low.

Table 2. Methods and risk of insider threat.

Method	Description	Human Factor
Unintentional Insider	An authorized user accidentally performs an action that compromises information assets.	Motive: None Opportunity: Medium Capability: Low
Insider Social Engineering	Psychological manipulation of another insider to disclose or perform actions to harm organizations information assets.	Motive: High Opportunity: Low Capability: Low
Insider Fraud	Using authorized access for personal gain by viewing, creating, modifying, deleting, or sharing information assets.	Motive: High Opportunity: High Capability: Medium
Insider IP Theft	An authorized user engages in espionage or stealing information like source code, business plan, strategic plans, product information, or customer information.	Motive: High Opportunity: High Capability: Medium
Insider IT Sabotage	Using IT experience and knowledge to launch an attack on an individual or organization	Motive: High Opportunity: Low Capability: Low

3.2. Insider threat types

An insider may act in a manner they are not supposed to, accidentally, deliberately, or forcibly, and the threat can be challenging to predict (Prabhu & Thompson, 2020). Understanding the types of insider threats to the organization is crucial to develop the right mitigation strategies.

The focus for insider threat is generally on the motive or the intentional action of the breach (Hadlington, 2018) and described as unintentional and intentional (Crossler et al., 2013). One of the dominant themes used for the threat classification is the malicious intent associated with the action and described as accidental, non-malicious, and malicious (Kraemer & Carayon, 2007; Van Den Bergh & Njenga, 2016; Willison & Warkentin, 2013). Another dominant theme is the combination of the malicious intent and the intentional action and describe the insider as accidental, unintentional non-malicious (negligent), intentional non-malicious (mischievous, well-meaning), and malicious (Carroll et al., 2014; Prabhu & Thompson, 2020; Wall, 2013). Other classifications use technical skills and their intent to harm (Stanton et al., 2005). The predominantly used insider threat types are briefly described below.

- Malicious: Causing harm or increasing the probability of future harm to the information systems with malicious intent (CERT, 2018). The insider has a motive to harm and makes a conscious decision to act inappropriately. For example, acts of leaking information to competitors, sabotaging IT networks, and using privileges for personal benefit.
- Mischievous: Intentional misuse of privileges without any malicious intent (Carroll et al., 2014; Prabhu & Thompson, 2020; Stanton et al., 2005). The insider is aware of the security risks but does not follow the prescribed procedures. Their actions generally make their job easier by having a workaround such as using unauthorized applications or media. For example, downloading illegal software applications to finish a job quicker.

- Negligent: Deliberate omission of information security measures without malicious motive or misuse of privileges (Carroll et al., 2014; Prabhu & Thompson, 2020; Stanton et al., 2005). The insider ignores the security policy because of the naïve perception that their omissive behavior is of low risk, for example, by not following the password policies or failing to update software patches.
- Accidental: An unexpected act without malicious motive or deliberate intent (Kraemer & Carayon, 2007; Willison & Warkentin, 2013). The insider has no motive to harm and makes no conscious decision to go against the prescribed policies. The acts are generally an error due to being unfocused or rushing things. For example, deleting the wrong file or sending sensitive e-mails to the wrong person. Sometimes, they legitimately follow instructions, but the instructions could result in unintended effects.

Figure 1 provides a quick summary of the characteristics of the different types of insiders identified above.

Some studies, such as Willison and Warkentin (2013), Aurigemma and Mattson (2014), and Prabhu and Thompson (2020), show the characteristics of insider types as a continuum rather than distinct as an individual's behavior is a gradient rather than distinct. The motivation that differentiates a malicious insider from a non-malicious insider may not always be evident for a breach.

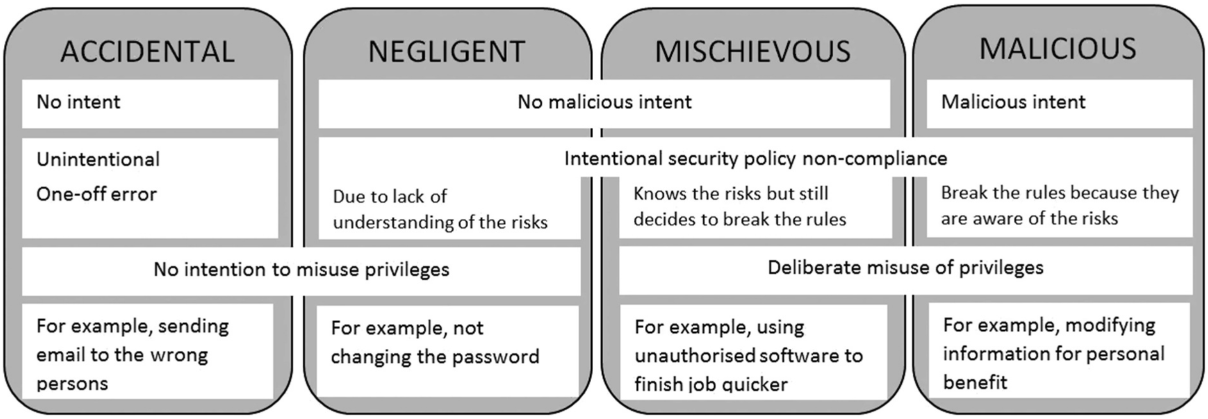
3.3. Motivations for insider breaches

A crime is only possible when a motivated attacker interacts with a vulnerable target (Ngafeeson, 2010). To understand the motivation for insider attacks from a cybersecurity perspective, several researchers have investigated an insider's security behavior and tendencies to violate policies.

Financial motivations drive a majority of cyber incidents (Ghafir et al., 2016; Goldman & McCoy, 2016) and can take the form of financial fraud, information theft, and selling sensitive information to outsiders.

The personal characteristics of an individual can play a significant role in their security behavior. Shaw et al. (1999) identify six personal characteristics that are likely to have implications for malicious insider breaches as a sense of entitlement (status-related desire for revenge), history of frustration (dislike of authority), computer dependency (challenging computer security systems), ethical flexibility (lack of moral inhibitions), reduced loyalty (lack of sense of belonging with their employer), and lack of empathy (inability to see effects of the impact on others). Similarly, Dupuis and Khadeer (2016) list trait effect as part of the insider profile as personality (feeling of superiority, lack of remorse), emotions (disgruntlement), financial status (stress to overcome debt), social theories, business factors (offshore work, remote offices), and cultural factors (organizational and regional culture).

An individual's technical knowledge and information seeking skills can play a role in their security behavior (Anwar et al., 2017) as they are



ACCIDENTAL	NEGLIGENT	MISCHIEVOUS	MALICIOUS
No intent	No malicious intent		Malicious intent
Unintentional One-off error	Intentional security policy non-compliance Due to lack of understanding of the risks	Knows the risks but still decides to break the rules	Break the rules because they are aware of the risks
No intention to misuse privileges		Deliberate misuse of privileges	
For example, sending email to the wrong persons	For example, not changing the password	For example, using unauthorised software to finish job quicker	For example, modifying information for personal benefit

Figure 1. Classification of insiders.

dominated by an interest in exploring networks and hack into computers as a challenge (Shaw et al., 1999), for innocent action, fun, or criminal intentions (Hunker & Probst, 2011). Also, it is noted that younger generations are willing to take higher risks. This, combined with greater computer literacy, the younger generations exhibit the willingness to push the rules to the limit (Jones & Colwill, 2008).

Sasse et al. (2007) present organizational factors such as growing integration of supply chains, outsourcing, off-shore work, and virtual organizations. Unaddressed discontent in the organization, recruitment by hostile outside entities, and infiltration of a malicious threat to a trusted person can also be reasons for an individual's security behavior (NAIC, 2008). High workload, complex security policies, and habitual bypassing of security mechanisms increase the chances of making a mistake and create opportunities for new types of attacks (Sasse et al., 2007). Metalidou et al. (2014) focus on the human factors that have severe implications in following security guidelines in place, namely lack of motivation to adapt secure behavior, lack of awareness of attacks, interpretations of the security guidelines, risky behavior, and inadequate knowledge to use technology.

Several factors motivate an individual to behavior to commit cybercrime or not. Some of the factors identified through literature are (1) personality – a sense of entitlement, feeling of superiority, ethical flexibility, lack of remorse, lack of empathy, and lack of loyalty, (2) financial needs – self-benefit or personal gains, (3) emotion – disgruntlement, personal and social frustration, stress, anger, revenge, and ego, (4) external loyalties – ideology, espionage, collusion, and recruitment from outsiders, (5) knowledge and skills – technical challenge, fun, action, mischief, out of curiosity, and criminal intention to use technology, (6) interconnectedness – extended insiders through outsourcing and off-shore work, competition from within, and reduced loyalty, and (7) organizational culture – lack of recognition, uncertainty and doubt of employment, anonymity, lack of accountability, lack of privilege, and neglecting employees. We summarize the factors that motivate human-centric breaches and illustrate them in Figure 2.

4. Discussion

While traditional areas of organizational security such as perimeter defense have matured and evolved, new human threats have emerged to take their place. This paper presented a primer on human factors in cybersecurity, with a specific focus on insider threats.

Our work has several theoretical implications as human factors are a crucial and sensitive aspect of cybersecurity. We highlight that organizations need to develop broader awareness of vulnerability and potential sources of attacks on their information systems. Recognizing the significant threat vector of insiders attempting to circumvent organizational information controls is an essential aspect of cybersecurity. Once organizations understand their areas of likely attacks, they will be in a better position to defend their systems. Unfortunately, human factors are not readily quantifiable, and thus a single solution will not apply to all situations. We attribute this to the multi-dimensional and multi-faceted nature of human behavior.

A further implication is an awareness of the alarming proposition when dealing with human-factor related breaches. Employees of an organization (i.e. insiders) may pose no less risk than outsiders. Furthermore, the unwitting insider, who may be tricked via social engineering, is another significant contributor within the context of human factors related breaches. Employees need to be trained to recognize attempts of manipulation, both through outsiders and through insiders. The neglect of the human factor as a threat is a direct consequence of focusing only on technical systems as targets and technology-based countermeasures in cybersecurity.

Many incident investigations reveal that changes in people's attitudes, behaviors, and actions can be warning signs of a probable attack. Often people reflect that they had noticed a change in the attacker's behavior, but the behavior was not reported to the authorities because they did not think of it as being significant or they did not know that it should be reported. The organization should educate its employees on the potential damage deviant acts can cause and educate employees to identify and report suspicious or deviant actions. When individuals cooperate and comprehend the reasons for the security restrictions, they will be more inclined

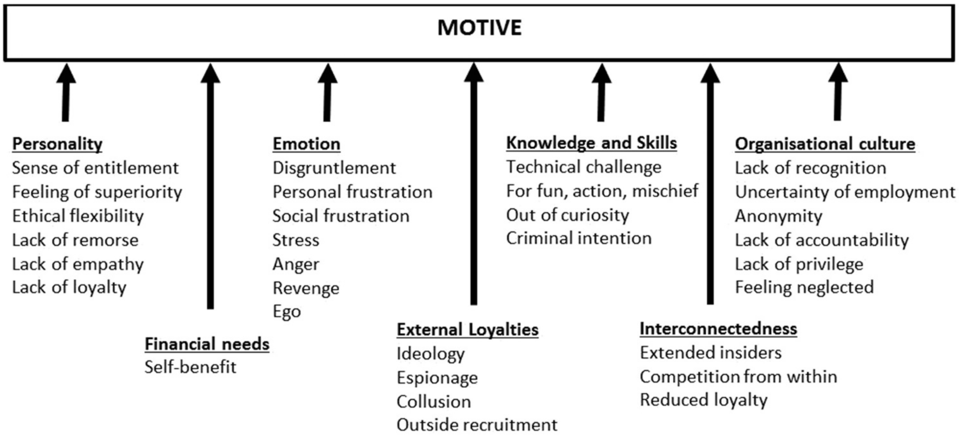


Figure 2. Factors motivating insider breaches.

to comply with policies and not seek workarounds. Actively involving employees in the development of information security policies can make them feel valued and contribute to the organization. Management should comprehend employees' workload and take responsibility for workload allocation, thereby reducing threats resulting from employee's tiredness or burn-out, resulting in unintentional harm to the organization. New systems should be designed without any assumption that everything within the organizational perimeter is trustworthy.

5. Conclusions

The threats to cybersecurity can only be addressed effectively by fully understanding the vulnerabilities, the threats, and the impact of a successful attack. Though no solution can fully eliminate human factor related threats to an organization, these can be managed to acceptable levels. The technical controls against attacks (such as access control, privileges, and auditing) should be combined with staff education, training, and awareness to be vigilant for human factors in cybersecurity. Human actions add a qualitative and often unpredictable dimension to threat models, rendering it infeasible to attempt to map out every possible human action and countermeasure.

Technical countermeasures alone are insufficient to address the range of possible insider threats. Therefore, the successful information security architecture should construct defenses to address the threats posed by the insider but remain vigilant against external threats. This uncertainty and shift away from the well-understood technical countermeasures may be possibly daunting for the non-expert. It is hoped that this brief primer will stimulate more interest in research and practice in this area, especially at the valuable intersection of technology and human behavior.

Notes on contributor

Sunitha Prabhu is a Senior Tutor at the University of Waikato, School of Computing and Mathematical Sciences, New Zealand. She completed her Masters in Computing and Mathematical Sciences specializing in Mathematics and is currently pursuing her PhD in Information Systems and Cybersecurity. With over 20 years of experience teaching Computer Science to tertiary students in New Zealand, her research interests include mathematics education, information security, and cybersecurity.

Nik Thompson is an Associate Professor in Information Systems at Curtin University, Australia. He holds MSc and PhD degrees and works in the area of Computer Security and Information Systems. His research interests include privacy, human-computer interaction, and information security. His work has appeared in various journals, including the Journal of the Association for Information Science and Technology, Computers & Security, and Behavior and Information Technology. For more information, please visit https://www.nikthompson.com

ORCID

Sunitha Prabhu http://orcid.org/0000-0002-8743-5984

References

Agrafiotis, I., et al. (2016). *Validating an insider threat detection system: A real scenario perspective. Paper presented at the 2016 IEEE Security and Privacy Workshops (SPW).*

Agrafiotis, A. Erola, J. Happa, M. Goldsmith, and S. Creese, "Validating an insider threat detection system: A real scenario perspective," in Proc. of the (2016) IEEE Security and Privacy Workshops (SPW'16), San Jose, California, USA. IEEE, May 2016, pp. 286–295.2016

Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., Furnell, S., Hayat, A., & Khurram Khan, M. (2015). Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, *48*, 44–57. https://doi.org/10.1016/j.jnca.2014.10.009

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees‘ cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Aurigemma, S., & Mattson, T. (2014). *Do it OR ELSE! Exploring the effectiveness of deterrence on employee compliance with information security policies. Paper presented at the AMCIS 2014 Conference Proceedings, Savannah, Georgia, USA*. August 2014.

Carroll, T. E., Greitzer, F. L., & Roberts, A. D. (2014). Security informatics research challenges for mitigating cyber friendly fire. *Security Informatics*, *3*(1), 13. https://doi.org/10.1186/s13388-014-0013-5

CERT. (2016). *Common sence guide to mitigating insider threat* (*Fifth Edition*). The CERT Insider Threat Center, Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf

CERT. (2018). *Common sense guide to mitigating insider threat (Sixth Edition)*. The CERT Insider Threat Centre, Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf

Chabinsky, S. R. (2010). Cybersecurity strategy: A primer for policy makers and those on the front line. *J. Nat'l Sec. L. & Pol'y*, *4(1)*, pp. 27-40. https://jnslp.com/wp-content/uploads/2010/08/04_Chabinsky.pdf

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

Crossler, Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90–101. https://doi.org/10.1016/j.cose.2012.09.010

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H.,& Stephenson, R. J. (2019, September). Human Risk Factors in Cybersecurity. In Proceedings of the 20th Annual SIG Conference on Information Technology Education. Tacoma, WA, USA. October 2019, pp 87-92.

Dupuis, M., & Khadeer, S. (2016). *Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. Paper presented at the Proceedings of the 5th Annual Conference on Research in Information Technology, Boston, MA, USA, 2016, pp. 35-40.*

Elmrabit, N., Yang, S.-H., & Yang, L. (2015). *Insider threats in information security categories and approaches. Paper presented at the 2015 21st International Conference on Automation and Computing (ICAC), Glasgow, UK, Sep. 2015, pp 1-6.*

Giandomenico, N., & Groot, J. D. (2018). *Insider vs. outsider data security threats: What's the greater risk?*. Digital Guardian's Blog, Digital Guardian. https://digitalguardian.com/blog/insider-outsider-data-security-threatshttps://securitypolicylaw.syr.edu/wp-content/uploads/2015/06/Goldman_Deterring_Financially_Motivated_Cyber-Crime-DRAFT.pdf

Greenberg, A. (2015). *Human error cited as leading contributor to breaches, study shows.* SC Magazine, CyberRisk Alliance. https://www.scmagazine.com/home/security-news/human-error-cited-as-leading-contributor-to-breaches-study-shows/

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider.

Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, *2* (1), 4–27.http://isyou.info/jowua/papers/jowua-v2n1-1.pdfhttps://doi.org/10.1109/CIC48465.2019.00047

Jones, A., & Colwill, C. (2008). *Dealing with the malicious insider*. Paper presented at the Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia.

Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied Ergonomics*, *38*(2), 143–154. https://doi.org/10.1016/j.apergo.2006.03.010

Lacombe, Y. (2017). *What is the greatest vulnerability in cyber security today? Vircom*. https://www.vircom.com/blog/greatest-vulnerability-cyber-security-today/

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151–171. https://doi.org/10.2308/ajpt-52593

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

NAIC, N. I. A. C. (2008). *The insider threat to critical infrastructures*. The National Infrastructure Advisory Council (NAIC), Department of Homeland Secirity (DHS). https://www.cisa.gov/sites/default/files/publications/niac-insider-threat-final-report-04-08-08-508.pdf

Ngafeeson, M. (2010). Cybercrime classification: A motivational model. , Dallas, Texas.

Nobles, C. (2019). Establishing human factors programs to mitigate blind spots in cybersecurity. In proceedings of the fourteenth Midwest Association for Information Systems Conference, Oshkosh, Wisconsin, May 2019.

Orshesky, C. M. (2003). Beyond technology–the human factor in business systems. *Journal of Business Strategy*, *24*(4), 43–47. https://doi.org/10.1108/02756660310494872

Privacy Act, N. Z. (2020). *Privacy Act NZ 2020*. Office of Privacy Commissioner, New Zealand. https://www.privacy.org.nz/privacy-act-2020/privacy-act-2020/

Proctor, R. W., Schultz, E. E., & Vu, K.-P. L. (2009). Human factors in information security and privacy. Gupta J.N.D. and Sharma S. (Eds). In *Handbook of research on information security and assurance* (pp. 402–414). IGI Global. DOI: 10.4018/978-1-59904-855-0.ch035

Prabhu, S., & Thompson, N. (2020). A Unified Classification Model of Insider Threats to Information Security. *ACIS 2020 Proceedings,Wellington,* NZ. 40. https://aisel.aisnet.org/acis2020/40

Sasse, M. A. et al. (2007). Human vulnerabilities in security systems. *Human factors working group*, *Cyber security KTN human factors white paper*

Shaw, E. D., Post, J. M., & Ruby, K. G. (1999). Inside the mind of the insider. *Security Management*, *43*(12), 34–42. https://www.asisonline.org/security-management-magazine/monthly-issues/archive/1999/December

Spring, J. M., & Illari, P. (2019). *Review of human decision-making during computer security incident analysis* (Vol. 1903, pp. 10080). arXiv preprint arXiv.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Van Den Bergh, M., & Njenga, K. (2016). *Information security policy violation: The triad of internal threat agent behaviors. Paper presented at the Proceedings of the 1st International Conference on the Internet, Cyber Security, and Information Systems (ICICIS),*Gabarone, Botswana.

Wall, D. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, *26*(2), 107–124. https://doi.org/10.1057/sj.2012.1

Walton, R., & Limited, W.-M. (2006). Balancing the insider and outsider threat. *Computer Fraud & Security*, *2006*(11), 8–11. https://doi.org/10.1016/S1361-3723(06)70440-7

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1–20. https://doi.org/10.25300/MISQ/2013/37.1.01