A Security Awareness Program for PCI DSS Compliance

Implementation and Legal and Ethical Issues to Be Considered

Fintech organizations that provide payment solutions to merchants, banks and financial institutions have a strict requirement to maintain security and regulatory compliance. Because they cater to the credit card industry, which processes sensitive cardholder data, they should be Payment Card Industry Data Security Standard (PCI DSS)-compliant, and controls should be in place for data loss prevention (DLP). It is necessary to adhere to PCI DSS to protect sensitive cardholder data.[1] PCI DSS is mandated by card schemes (payment networks that facilitate the processing of card payments such as Visa, Mastercard, American Express) and administered by the Payment Card Industry Security Standards Council (PCI SSC). Noncompliance with PCI DSS could result in heavy penalties imposed by schemes. As part of PCI DSS compliance, organizations must have a security awareness program in place to adhere to PCI DSS regulations and protect against security threats. However, just having an awareness program may not be effective. Ensuring that employees understand the legal and ethical issues of not complying with regulations and best practices in security is essential to having an effective awareness program. A security education training and awareness (SETA) program will be more effective if it not only outlines what is expected (knowledge) but also provides an understanding of why this is important (attitude).[2]

What Is PCI DSS?

PCI DSS governs the handling of cardholder data and establishes minimum data protection requirements for all organizations involved in payment card processing.[3] It is governed by the PCI SSC, which is composed of five members: American Express, Discover, JCB International, Mastercard and Visa. It is applicable to merchants, transaction processors, acquirers, issuers and service providers. Any organization, small or large, that stores, processes or transmits cardholder data or sensitive authentication data needs to meet 12 requirements:[4]

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need-to-know.

YASMIN RAZACK | PH.D., CISA, ISO 20000 LI, ITIL V3, Lean Six Sigma Black Belt, NLP, PMP, SaFE Agilist

Has more than 25 years of experience in the IT, airline and fintech industries. Razack is responsible for setting up service management and operational risk management strategy and standards, leading incident investigations and resolution, and executing various awareness and training programs. In her recent roles, she headed the change management division of a leading fintech enterprise in the Middle East and a global airline based out of Dubai, UAE. She is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Project Management Institute (PMI). She can be reached at yasminrazack65@gmail.com.

TIMOTHY SORBER | PH.D., DCS, PMP, ITIL V3

Has more than 35 years of experience in IT and enterprise architecture with special expertise in the US Department of Defense Architecture Framework (DODAF). He is a professor of information assurance at the American National University (Salem, Virginia, USA) and the University of Fairfax (Vienna, Virginia, USA). He has more than five years of experience mentoring doctoral students in cybersecurity and information assurance. He is an expert in the operational level of war organization processes across a variety of global missions, including Integrated Air and Missile Defense (IAMD), Cyberspace Command and Control, Joint Suppression of Enemy Air Defenses (JSEAD), and Command and Control in Degraded or Denied Environments (C2D2E). He can be reached at tsorber@an.edu.

8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

> "The ambiguity of PCI DSS is that stakeholders who need to be made aware are not explicitly mentioned in the document."

PCI DSS v. 3.2.1 describes in detail what organizations need to incorporate in their security plans to keep their data safe.[5] In addition, the PCI SSC has developed a prioritized approach to implement the standards. The prioritized approach mentions the areas in which awareness needs to be created.[6] The need to create awareness is mentioned for nine out of 12 requirements. The ambiguity of PCI DSS is that stakeholders who need to be made aware are not explicitly mentioned in the document published by the PCI SSC, which refers only to "all affected parties."[7] It is interesting to note that PCI SSC does not impose compliance with PCI DSS; instead, the individual schemes such as Visa or Mastercard determine the noncompliance penalties. The consequences of noncompliance include fines that vary based on what the schemes impose and termination of network participation. Further, PCI SSC v. 3.2.1 does not mention how awareness needs to be created or the proposed delivery methods for creating awareness in the security requirements.

Why Security Awareness?

To protect sensitive data, most organizations focus on technology first by deploying the latest antivirus tools, intrusion detection systems (IDS), virtual private networks (VPNs) and firewalls to guard against threats and attackers. The human element is often ignored.[8] People need to be made aware of basic threats arising from tailgating, phishing, social engineering, theft and malware. Technology should be supported by robust processes (i.e., governance frameworks), policies and, most important, people with the right skill sets and awareness.[9]

One of the requirements of PCI is the need for a clear, enforced security policy.[10] This means that all organizations accepting or processing payment transactions (from merchants, banks, payment processors, service and technology providers to commercial customers and cardholders) must inform all stakeholders adequately about PCI requirements and threats related to the payment industry. These stakeholders include management, executives and staff members who have any operational or technical role in processing the cardholder data, along with compliance officers, finance specialists, audit managers, credit analysts, system administrators and developers.

All employees need to be aware, at a minimum, of general security training tips pertaining to phishing, physical security, mobile device security and viruses.[11] They should also know the definition of cardholder data and sensitive authentication data (SAD) and understand their responsibilities to safeguard them. Depending on how the credit card information is normally collected (e.g., by phone, electronically, on paper), specific handling procedures should be implemented.

Insider Threats

Insider threats are internal users who may be authorized to use a system and, therefore, have the ability to attack it. Insider attacks may be intentional or accidental. They can come from poorly trained administrators who make mistakes or malicious individuals who intentionally compromise the security of systems. There has been an increase in insider threats from 2016 to 2018 (**figure 1**).[12] The Ponemon Institute *2018 Cost of Insider Threats Study* shows that the average cost of an insider-related incident is approximately US$513,000.[13]

Insider-related incidents can cost an organization up to US$8.76 million a year. The *2019 Cost of Cybercrime Study* indicates that the average cost of a malicious insider attack rose 15 percent from 2018 to 2019.[14] Moreover, the insider threat statistics in 2019 show that organizations should pay more attention to regular employees because:

- Privileged accounts are usually better monitored and secured than accounts of regular users.
- Although regular employees have access to some sensitive data, they often are not well monitored and sometimes lack basic cybersecurity training.

Research carried out in 2020 found that organizations in the Middle East experienced the most insider incidents, and organizations in the Asia-Pacific region had the fewest incidents.[15] **Figure 2** shows the frequency of insider incidents in the four regions represented in the research. In all regions, employee or contractor negligence occurred most frequently. North America and the Middle East are most likely to experience credential theft.

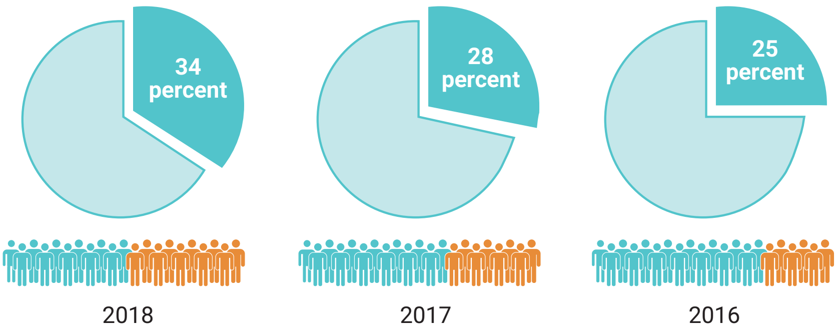
The five most common types of malicious insiders include:[16]

1. **Careless workers**—These are employees who ignore enterprise cybersecurity policies, misuse data and install unauthorized applications (apps). This usually happens because it is easier for them to work when ignoring safety rules. Careless employees have no malicious intent, but their inadvertent actions may cause devastating security breaches.
2. **Inside agents**—These are employees recruited by external parties to steal or corrupt an organization's data.
3. **Disgruntled employees**—These employees may take revenge on an organization by destroying or selling its data or disrupting business activity.
4. **Malicious insiders**—These are employees who deliberately misuse sensitive enterprise information for personal gain.
5. **Third-party users**—These are vendors or business partners who compromise cybersecurity because of negligence, data misuse, malicious intent or accidents. In some cases, third-party contractors are not aware of clients' cybersecurity policies and break them unknowingly.

Attacks from these types of users can have a significant impact on the organization.[17] According to the US National Institute of Standards and

FIGURE 1

Growth of Insider Attacks

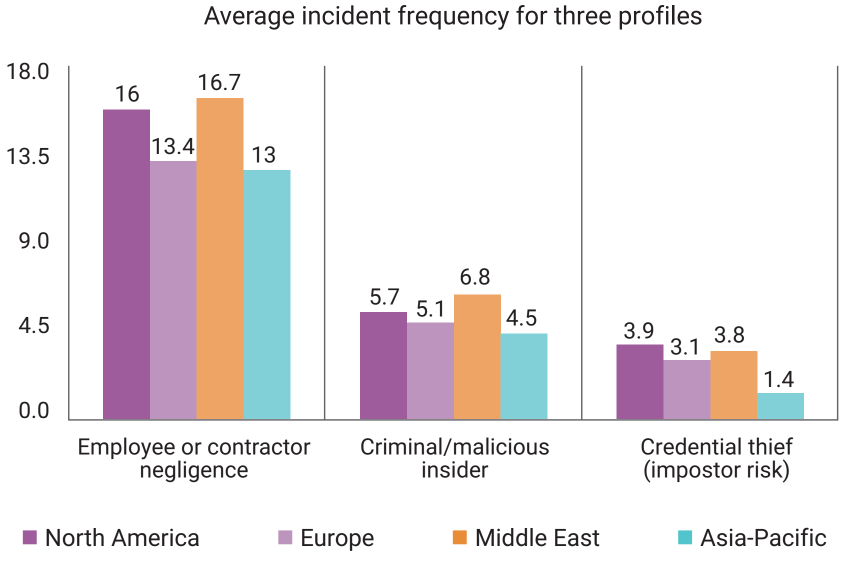


* Data provided by the *2017–2019 Verizon Data Breach Investigations* reports

Source: Ekran, "Insider Threat Statistics for 2020: Facts and Figures," USA, 2019, *https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures*. Reprinted with permission.

FIGURE 2

Frequency of Insider Incidents



Source: Ekran, "Insider Threat Statistics for 2020: Facts and Figures," USA, 2019, *https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures*. Reprinted with permission.

> “Lack of information security awareness, ignorance, negligence, apathy, mischief and resistance are often at the root of user mistakes.”

Technology (NIST), threat actions caused by insiders include employee assault; blackmail; browsing of proprietary information; computer abuse; fraud and theft; information bribery; input of falsified; corrupted data; interception; malicious code (e.g., virus, trojan horses); sale of personally identifiable information (PII); system bugs; intrusion; sabotage; unauthorized system access.[18]

It is noteworthy that social engineering is used as a vector to propagate malicious programs, which is why it is important for employees to be aware of social engineering malware trends and tactics.[19] Implementation of periodic awareness education can reduce the risk of employees falling victim to socially engineered malware tactics. Employers should develop an ongoing, comprehensive information security program that caters to employees at all levels.

Importance of a Security Education Training and Awareness Program

A SETA program is defined as a program aimed at reducing the number of security threats or breaches that occur due to lack of security awareness.[20] A SETA program aims to improve employees’ capabilities in reacting to threats by improving their skill sets and their understanding of information security policy so that good practices can be promoted in the organization.[21] Ultimately, this helps protect information assets and data to maintain confidentiality, integrity and availability.[22] Security awareness is the combination of both knowing and doing something to protect business information assets.[23] When an organization’s employees are cybersecurity aware, it means they understand what cyberthreats are, the potential impact a cyberattack can have on their business, and the steps required to reduce risk and prevent cybercrime from creeping into their online workspace.

Many consider the user to be the weakest link in information security.[24] Employee negligence and inside breaches are often the main causes of security threats. Lack of information security awareness, ignorance, negligence, apathy, mischief and resistance are often at the root of user mistakes. There is a strong correlation between information security awareness and user behavior related to Internet use, mobile computing and email use.[25] Educating employees through cybersecurity awareness programs is not a one-time activity and needs to be repeatedly reinforced using multiple methods to continually benefit the organization.[26]

Security Awareness Delivery Methods

Learning methods for information security awareness should include ways to clarify threats, vulnerabilities, attacks and possible damage, and they should define the main values of information security and data protection.[27] Awareness campaigns often use presentations supported by flyers, posters, brochures or web-based trainings (WBTs) to transfer knowledge, and employees often may complete the trainings at a place and time of their choosing. Along with knowledge transfer, awareness-raising activities include marketing elements, which convey messages by capturing the attention of employees through appeals to their emotions. In addition to the theoretical approach to knowledge transfer and the promotional approach of emotional marketing, a more comprehensive method (**figure 3**) of eliciting emotions and social participation helps create lasting information security awareness and encourage security-related behaviors.[28]

Despite efforts to increase information security awareness, research is scant regarding effective information security awareness delivery methods. Some methods include contextual training and embedded training. Research was also conducted on the use of text-based, game-based and video-based delivery methods with the aim of determining user preferences. One study suggests that a combined delivery method is better and more successful than individual security awareness delivery methods.[29]

Legal and Ethical Issues to Be Addressed During Implementation

When creating a security awareness program, an organization must ensure that employees are aware of a number of legal and ethical issues.[30]

LOOKING FOR MORE?

- Read *Practical Guide to the Payment Card Industry Data Security Standard.* *www.isaca.org/payment-card-industry*
- Learn more about, discuss and collaborate on information and cybersecurity in *https://engage.isaca.org/onlineforums*

Legal Issues

Legal liability may arise from not implementing best security practices, such as developing and maintaining a security program, developing security policies and procedures, monitoring security controls and using performance metrics for tracking improvement, assigning ownership for security activities (e.g., a compliance manager for regular compliance review and action), and detecting and responding to security incidents. Not complying with these regulations may involve penalties. The fines can be up to US$100,000 per month.[31] When organizations train their employees on security best practices and regulatory compliance, it can help avoid legal issues and fines. Organizations should train their employees to ensure that they know what they need to do to comply with information security rules and industry regulations.[32]

Ethical Issues

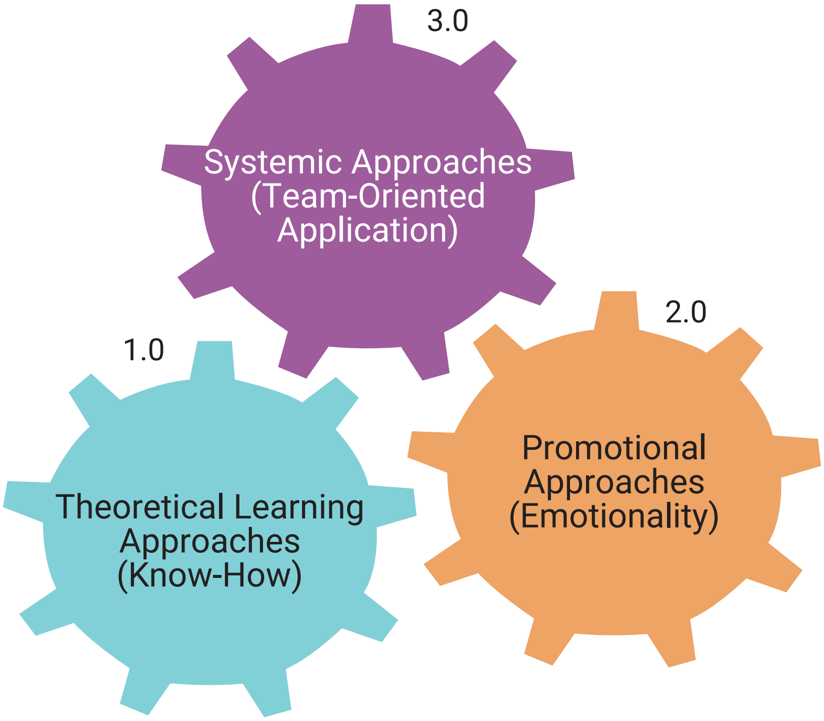
There are a number of ethical issues faced by IT security professionals on a day-to-day basis.[33] For example, an employee may come across a document that shows the employer is violating government regulations and laws. Does the employee have a moral responsibility to highlight the violation or is the employee ethically bound to respect the employer's privacy? What would be the difference if the employee had signed a nondisclosure agreement when accepting the job? As a security consultant, it may be easy to make a client spend more than is required by stoking fear about risk. Some consultants may take payments from equipment manufacturers for persuading their clients to purchase the manufacturers' products or to patronize organizations in which they hold stocks.

> "There are no standard bodies that have established a code of ethics for IT security."

Another scenario could involve a client asking to cut off a few security measures to save costs. The security consultant knows that sensitive information will be at risk and the organization will fall behind in compliance. Should the consultant go ahead and configure the settings that are less secure, violating compliance, or absorb the costs to provide a comprehensive solution?

FIGURE 3

ISA Delivery Methods


3.0
Systemic Approaches (Team-Oriented Application)
2.0
Promotional Approaches (Emotionality)
1.0
Theoretical Learning Approaches (Know-How)

Source: Scholl, M.; "Information Security Awareness in Public Administration," *Public Management and Administration*, 29 August 2018, *www.intechopen.com/chapters/59667*. Reprinted with permission.

Actions such as falling prey to phishing attacks or inadvertently giving access to an organization's information can be avoided with the help of PCI DSS policy awareness training.[34] All staff, including consultants and temporary staff working on cardholder data, should be aware of the importance of data and the need to protect them. However, the behavior of employees and their responses to ethical scenarios are not governed by regulations such as PCI DSS. Responses often depend on the individual and the influence of an organization's culture.

An employee's intention to behave ethically or unethically is strongly related to the context of the individual's perceived organizational environment and influenced by that individual's moral obligation toward performing an act.[35] There are no standard bodies that have established a code of ethics for IT security. However, organizations such as the Association for Computing Machinery (ACM) have developed their own codes of ethics and professional conduct,[36]

> “Getting users to report and respond correctly to security incidents rather than covering them up is one of the biggest challenges faced by management.”

which can serve as guidelines for individuals and other organizations. Organizations can tailor their security awareness training policies appropriately to address the ethical and legal issues. However, culture does play an important part in improving moral values and beliefs of employees in an organization.[37] Management can also be role models and foster a culture of information security, where security is considered as everybody’s responsibility, not just the responsibility of the information security department.

The Critical Role of Top Management and an Organizational Culture

Research has stressed the importance of top management in influencing the security compliance behavior of employees.[38] Through hypothesis testing, top management participation has been found to strongly influence organizational culture, which, in turn, impacts employees’ attitudes toward and perceived behavioral control over compliance with information security policies. Employees account for more information security disruptions than outside attacks, and they are potentially more dangerous to organizations because of their working knowledge of their organizations. Plus, employees’ noncompliance to security policies can be disastrous for an organization, often making them the weakest point in any information security model.[39] Establishing an awareness program can help organizations avoid these pitfalls, but the influence and management of the organizational culture by top management can also shape and guide employee behavior via shared values and commitment to the organization.

Creating a culture around cybersecurity awareness in the workplace does not mean that the risk of data theft or cybercrime can be completely eradicated.[40] As new strains of malware grow, enterprises need to ensure that they are implementing appropriate security measures, educating their employees and eliminating any weaknesses that make them vulnerable to attacks, as human error is an exploit that can lead to fines and severe business damage.

The characteristics of employees (roles and learning styles), the compliance with current policies, the state of the security culture, and the mission, vision and strategic planning of the organization should be considered when setting up a security culture development plan.[41] When developing a security awareness plan, a senior manager should be identified to champion the program, and members from the IT, human resources (HR), marketing, legal and security teams should actively participate in the program. Those who are selected to deliver security trainings should focus on employees’ higher-order thinking skills, such as evaluating, judging, creating, and formulating ideas and work to meet people’s learning styles.

Implementation Issues Faced by Management

When creating a security awareness program, management faces a number of issues from the planning phase to the monitoring and evaluating phase.

- **Lack of resource, timing and support**—The lack of ability to execute the program due to resource, time and support is the biggest issue that management faces.[42] The resources allocated for a security awareness program can get caught up with other operational responsibilities and become unable to be used to execute the program as planned. Budgets also get prioritized to business-critical initiatives, and getting them approved to be used for these types of programs can be difficult.
- **Geographically distributed employees**—It is challenging to get all employees engaged on the program if they are geographically distributed, especially in a large organization.[43] For the training to be effective, different time zones, preferred training methods and reinforcement strategies have to be considered.[44] The program should cater to off-site employees, remote workers, shift personnel and employees whose roles prevent them from having regular schedules. Also, cultural differences with people from different countries have to be taken into account.
- **Training content and delivery mechanisms**—Management needs to decide if the training should be conducted in-house or outsourced and whether it should be instructional or self-taught. Often when addressing the training needs of large

workforces, just one or two methods of training may not be effective. Posters, screensavers and warning banners; computer-generated alerts; organizationwide email messages; web-based sessions; computer-based sessions; teleconferencing sessions; in-person instructor-led sessions; simulations; and seminars are some of the techniques that can be used for the program.[45] Other things to consider are keeping the topics relevant, keeping the topics current and determining the frequency of training.

- **Behavior modification**—The ultimate goal of a security awareness program is to change the attitudes and behavior of employees.[46] Imparting knowledge is not enough. Getting users to report and respond correctly to security incidents rather than covering them up is one of the biggest challenges faced by management. Hence, training programs can measure the effectiveness of the training by changing employee attitudes.

Conclusion

People are often considered the weakest link in an organization's cybersecurity defenses. Hence, cyberattackers often use techniques such as spear phishing, social engineering, ransomware and malware to target employees of an organization, who are often easy to exploit. Although a great deal of effort typically goes into improving the existing security infrastructure, ignoring HR leaves a significant gap in an organization's cyberdefense strategy. Therefore, educating employees through cybersecurity awareness programs can bolster an organization's cybersecurity efforts. Cybersecurity awareness training is not a one-time activity, and it should be repeatedly reinforced through multiple methods.

Several groups in an organization, from the risk management team to HR to third-party vendors, should be involved in security awareness training. The training cannot be a one-size-fits-all solution and should be customized according to the audience. It should inculcate a sense of responsibility and accountability in employees so that the organization is safe from attacks that exploit the human factor. As part of PCI DSS compliance, organizations must have a security awareness program in place to adhere to PCI DSS regulations and protect against security threats. Legal and ethical issues must also be addressed appropriately by organizations and included in the training to help employees better understand the related moral values and ethics and legal implications of not following security best practices and policies. Top management and organization culture have critical roles in making the awareness program more effective and overcoming challenges in implementing the program. Having a security awareness program is no longer optional for organizations. Its return on investment is high, and it is a vital part of any information security plan. Security awareness programs can act as human firewalls if implemented effectively.

> "As part of PCI DSS compliance, organizations must have a security awareness program in place to adhere to PCI DSS regulations and protect against security threats."

Endnotes

[1] Parker, A. M.; "An Introduction to PCI DSS," Cryptomathic, 23 March 2018, *www.cryptomathic.com/news-events/blog/an-introduction-to-pci-dss*

[2] Pattinson, M.; *et al.*; "Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers and Security,* May 2014, *https://www.researchgate.net/publication/259991932_Determining_Employee_Awareness_Using_the_Human_Aspects_of_Information_Security_Questionnaire_HAIS-Q*

[3] Eversheds Sutherland, "Legal Alert: PCI DSS—What It Is and Why It Is Relevant to Your Business," 4 February 2016, *www.lexology.com/library/detail.aspx?g=94f604cc-acac-4d26-ac74-b9e329db1067*

[4] Payment Card Institute Security Standards Council (PCI SSC), *PCI Data Security Standard (DSS) Requirements and Security Assessment Procedures*, v. 3.2.1, May 2018, *www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1629395159708*

5 Payment Card Institute Security Standards Council (PCI SSC), *The Prioritized Approach to Pursue PCI DSS Compliance*, May 2016, *https://www.pcisecuritystandards.org/documents/Prioritized-Approach-for-PCI_DSS-v3_2.pdf*

6 *Ibid*.

7 *Ibid*.

8 Chen, X.; L. Chen; D. Wu; "Factors That Influence Employees' Security Policy Compliance Behavior: An Awareness-Motivation-Capability Perspective," *Journal of Computer Information Systems*, vol. 58, iss. 4, 27 December 2016, *www.tandfonline.com/doi/abs/10.1080/08874417.2016.1258679*

9 Dutton, J.; "Three Pillars of Cybersecurity," IT Governance, 26 September 2017, *www.itgovernance.co.uk/blog/three-pillars-of-cyber-security*

10 Brecht, D.; "PCI Security Awareness: Who Needs Training and Compliance?" *Infosec*, 2019, *https://resources.infosecinstitute.com/category/enterprise/securityawareness/compliance-mandates/who-needs-pci-training-in-my-organization/#gref*

11 *Ibid*.

12 Ekran, "Insider Threat Statistics for 2020: Facts and Figures," 28 January 2021, *www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures*

13 Ponemon Institute, *2018 Cost of Insider Threats: Global*, April 2018, *www.insiderthreatdefense.us/pdf/Ponemon%20Institute%202018%20Report%20-%20The%20True%20Cost%20Of%20Insider%20Threats%20Revealed.pdf*

14 Bissell, K.; R. LaSalle; P. Cin; *Ninth Annual Cost of Cybercrime Study, Accenture and Ponemon Institute*, 6 March 2019, *www.accenture.com/us-en/insights/security/cost-cybercrime-study*

15 Ponemon Institute, *2020 Cost of Insider Threats Global Report,* USA, 2020, *https://153j3ttjub71nfe89mc7r5gb-wpengine.netdna-ssl.com/wp-content/uploads/2020/02/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf*

16 *Op cit* Ekran

17 Conrad, E.; S. Misenar; J. Feldman; *CISSP Study Guide, 2nd Edition*, Elsevier, USA, 2012

18 National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, USA, December 2018, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf*

19 Abraham, S.; I. Chengalur-Smith; "An Overview of Social Engineering Malware: Trends, Tactics, and Implications," *Technology in Society*, vol. 32, iss. 3, August 2010, p. 183–196, *http://dx.doi.org/10.1016/j.techsoc.2010.07.001*

20 Whitman, M. E.; H. J. Mattord; *Management of Information Security*, Thomson Course Technology, Canada, 2004

21 Karyda, M.; I. Topa; "Identifying Factors That Influence Employees' Security Behavior for Enhancing ISP Compliance," 12th Trust, Privacy and Security in Digital Business International Conference, Valencia, Spain, September 2015, *www.researchgate.net/publication/281938225_Identifying_Factors_that_Influence_Employees'_Security_Behavior_for_Enhancing_ISP_Compliance*

22 Whitman, M. E.; H. J. Mattord; *Management of Information Security*, Cengage Learning, USA, 2017

23 CyberGuard Technologies, "The Importance of Cybersecurity Awareness," *www.ogl.co.uk/the-importance-of-cyber-security-awareness*

24 Scholl, M.; "Information Security Awareness in Public Administrations," *Public Management and Administration*, 29 August 2018, *www.intechopen.com/chapters/59667*

25 *Op cit* Pattinson *et al*.

26 Robinson, A.; *Using Influence Strategies to Improve Security Awareness*, SANS Institute, 25 October 2013, *www.sans.org/reading-room/whitepapers/awareness/influence-strategies-improve-security-awareness-programs-34385*

27 *Op cit* Scholl

28 *Ibid*.

29 Abawajy, J.; "User Preference of Cyber Security Awareness Delivery Methods," *Behavior and Information Technology*, vol. 33, iss. 3, 1 August 2012, *http://dx.doi.org/10.1080/0144929X.2012.708787*

30 Petkovic, M.; W. Jonker; *Security, Privacy, and Trust in Modern Data Management*, Springer, Germany, 2007

31 Yantz, M.; "PCI Compliance: Comprehensive Guide to Protect Your Customers and Brand," IT Support Guys, 7 November 2019, *https://itsupportguys.*

com/it-blog/pci-compliance-comprehensive-guide-to-protect-your-customers-and-brand/

[32] Bulgurcu, B.; H. Cavusoglu; I. Benbasat; "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, vol. 34, iss. 3, p. 523–548, *https://misq.org/information-security-policy-compliance-an-empirical-study-of-rationality-based-beliefs-and-information-security-awareness.html*

[33] Shinder, D.; "Ethical Issues for IT Security Professionals," *Computerworld*, 2 August 2005, *www.computerworld.com/article/2557944/ethical-issues-for-it-security-professionals.html*

[34] Bykara, S.; "How to Implement the Security Awareness Training for PCI Compliance," PCI DSS Guide, 26 April 2020, *https://www.pcidssguide.com/implementing-a-security-awareness-program/*

[35] Banerjee, D.; T. Cronan; T. Jones; "Modeling IT Ethics: A Study in Situational Ethics," *MIS Quarterly*, vol. 22, iss. 1, March 1998, *http://dx.doi.org/10.2307/249677*

[36] *Op cit* Schinder

[37] Choo, K-K. R.; "The Cyber Threat Landscape: Challenges and Future Research Directions," *Computers and Security*, vol. 30, iss. 8, November 2011

[38] Hu, Q.; T. Dinev; P. Hart; D. Cooke; "Managing Employee Compliance With Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decision Sciences Journal*, vol. 43, 2012, *http://130.18.86.27/faculty/warkentin/SecurityPapers/Newer/HuDinevHartCooke2012_DecSciencesForthcoming_TopMgmt_OrgCultureCompliance.pdf*

[39] *Ibid*.

[40] OGL Computer Services, "The Importance of Cybersecurity Awareness," CyberGuard Technologies, *https://www.ogl.co.uk/the-importance-of-cyber-security-awareness*

[41] Olivos, O.; "Creating a Security Culture Development Plan and a Case Study," Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance (HAISA), 2012, *https://pdfs.semanticscholar.org/138a/e5e508d6f9de7d010be17ebe0ad071b9d462.pdf*

[42] Spitzner, L.; "The Top Challenges Facing Security Awareness Programs," SANS, 17 March 2016, *https://www.sans.org/security-awareness-training/blog/top-challenges-facing-security-awareness-programs*

[43] Devry, J.; "The Challenges of Raising User Security Awareness," *Cybersecurity Insiders*, *https://www.cybersecurity-insiders.com/the-challenges-of-raising-user-security-awareness-2/*

[44] Brecht, D.; "The Components of Top Security Awareness Programs," *Infosec*, 15 April 2019, *https://resources.infosecinstitute.com/components-top-security-awareness-programs/#gref*

[45] *Ibid*.

[46] *Op cit* Devry