ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 4/25 (April)

The Human Factor in Cybersecurity: Threats & Opportunities

INTRODUCTION: WE NEED MORE FOCUS ON PEOPLE

1. The alarming prevalence of social engineering attacks (Fig. 1) has shown that humans are the easiest attack vector.

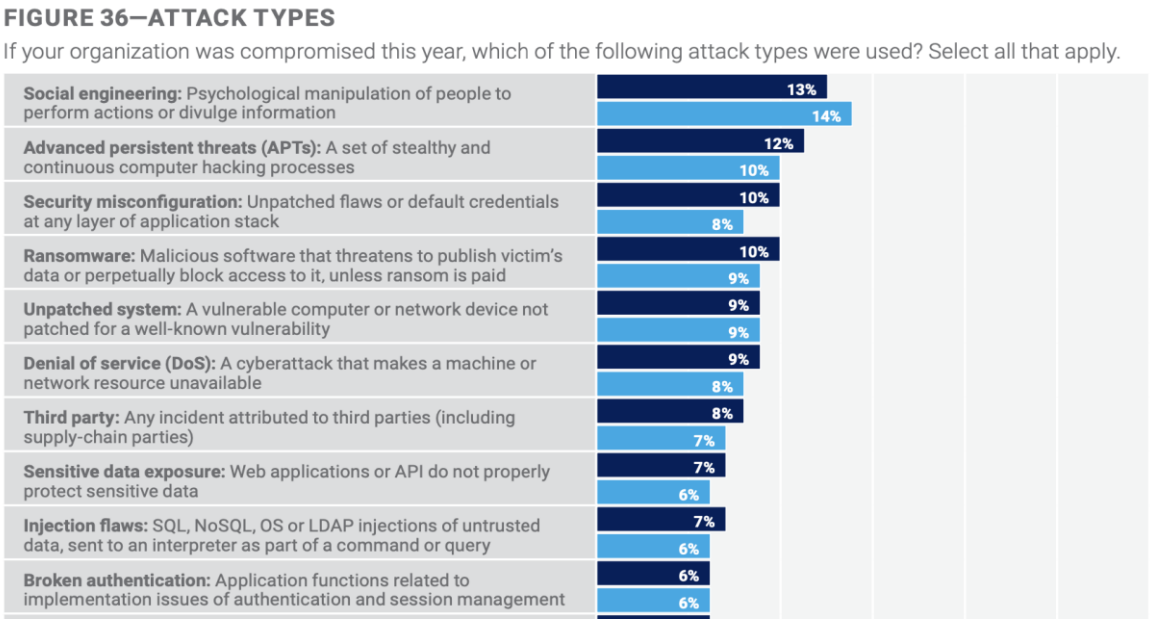

Fig. 1: Social engineering was the top cause of network compromises in both 2021 (light blue) and 2022 (dark blue) (Source: Information Systems Audit and Control Association's 2022 State of Cybersecurity Report)

2. Some of the most expensive data breaches also utilised social engineering tactics such as phishing and business email compromise (Fig. 2).

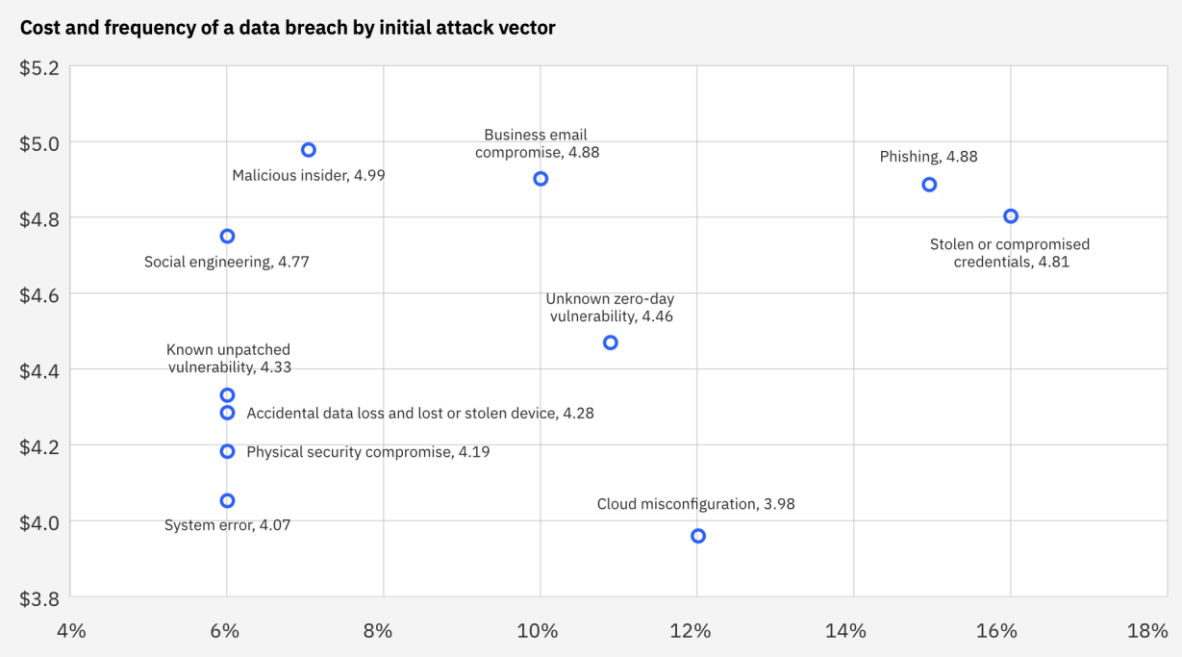

Fig. 2: Graph showing the cost and frequency of data breaches (Source: IBM 2024 Cost of a Data Breach Report)

3. Therefore, strengthening the human element in cyberspace is crucial. This digest will turn to cyberpsychology – defined by the British Psychological Society as the study of human thought and behaviour when humans interact with technology – for insights on how people contribute to cybersecurity failures, and how psychological concepts can be applied to strengthen the human element in cyberspace.

THE PSYCHOLOGY BEHIND CYBERSECURITY FAILURES

4. People unknowingly contribute to cybersecurity failures in various ways, whether it's clicking that phishing link, or failing to report suspicious computer behaviour. In deciding their course of action in cyberspace, people generally use two types of thinking: (a) fast, automatic thinking based on mental shortcuts; and (b) slow, deliberate thinking (Fig. 3).

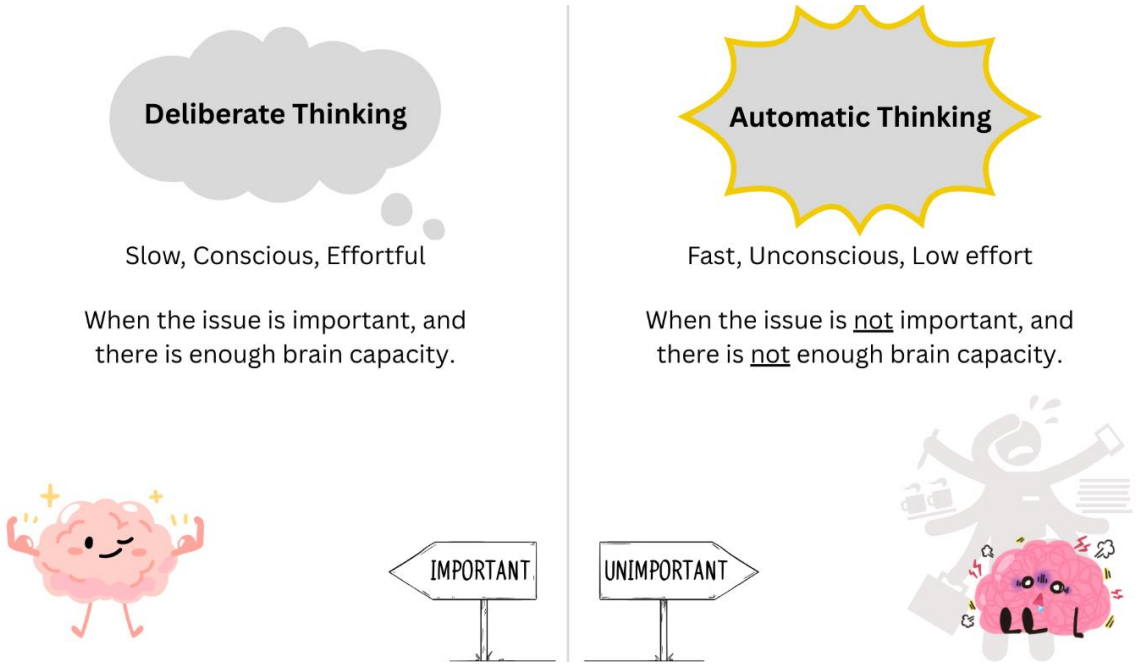

Fig. 3: Comparison of deliberate thinking (left) and automatic thinking (right)

5. Drivers that motivate people to use automatic thinking over deliberate thinking include:

a. Perceived Unimportance of Cybersecurity. People pay less attention to cybersecurity if it is irrelevant or unimportant to them. Availability bias also plays a role – if the information people can recall from memory suggests that they are at low risk of a cyberattack, people may downplay the importance of cybersecurity.

b. Cognitive Overload. When people are distracted by many other tasks, they are less likely to scrutinise potential threats.

6. As a result of automatic thinking, people may miss anomalies present in common social engineering attacks. For example:

a. Phishing Emails. Malicious actors impersonate individuals, such as government officers or institutions, in phishing emails. Users using automatic thinking may click on malicious email links without a second thought, because they assume that an email from someone authoritative, such as a supposed government officer or a government department, would be authentic. Malicious actors could also induce a false sense of urgency in phishing emails. Users using automatic thinking may pursue the

unimportant but "urgent" matter without a second thought, just to get the task done.

b. Business Email Compromise. Malicious actors impersonate business leaders and instruct subordinates to transfer money or share sensitive data. Subordinates, especially those who are occupied or overworked, may comply with their business leader's supposed instructions, even if it goes against company policy, because they assume that instructions from a higher authority would be authentic.

c. Pretexting. Malicious actors impersonate someone in a position of authority, fabricate plausible scenarios such as tax evasion charges, and instil fear or anxiety in victims. Under such circumstances, victims may assume that authority equals authenticity and readily disclose sensitive information without a second thought.

7. People who place more importance on good cyber hygiene, such as cybersecurity professionals, may use deliberate thinking to avoid falling for social engineering attacks. However, they may still fail to respond effectively to cybersecurity incidents due to other preconceived expectations. For example:

a. Schemas and Change Blindness. Schemas are mental frameworks that tell people what to expect in a given situation, and help people process information efficiently by focusing on key attributes of a given situation. However, schemas also cause people to expect that attacks follow a certain pattern. They may thus fail to recognise anomalies that deviate from expected patterns – a phenomenon known as change blindness – and overlook potential cybersecurity incidents.

b. Diffusion of Responsibility. People feel less responsible when they are part of a group, because they assume someone else will take action. As a result, entire teams may fail to respond even though each individual in the team is aware of the cyber threat.

8. These examples show the ease with which people's thoughts can lead to undesirable responses when performing everyday tasks in cyberspace. Some may not care about practising good cyber hygiene, while others may be overwhelmed

with too many tasks and fail to notice certain anomalies, or simply assume that their teammates will handle the cyber threat.

USING PSYCHOLOGY TO STRENGTHEN CYBERSECURITY

9. Individuals, organisations, and society can leverage psychological insights to improve cybersecurity practices.

10. Internal Locus of Control. Organisations can empower employees by fostering an internal locus of control – the belief that one has control over events and can directly impact cybersecurity rather than being a passive victim. Such individuals are more likely to believe that cybersecurity is relevant and important. They are also more likely to take personal responsibility for their cyber hygiene; for example, such individuals may proactively enable multi-factor authentication and exercise caution towards suspicious email attachments.

11. Positive Reinforcement. Organisations can also make use of positive reinforcement to encourage cybersecurity best practices. For example, rewarding employees who report phishing attempts or follow cybersecurity protocols increases the likelihood that these employees will continue to exhibit good cyber hygiene.

12. Social Norms. Finally, organisations can leverage social norms – acceptable workplace behaviours – to reinforce best practices in cybersecurity. People reference norms to decide how they should act, in order to fit into their workplace. When employees see cybersecurity as an expected and valued part of workplace culture – rather than an afterthought – they are more likely to adopt good cyber hygiene.

THE HUMAN ELEMENT CAN BE A STRENGTH

13. The hardware and software that humans use in cyberspace everyday are just tools. Cybersecurity is therefore not just a technological challenge – it is also a psychological one. While human behaviour and ways of thinking can contribute to vulnerabilities in cyberspace, psychological insights can also be applied to improve personal and organisational cyber hygiene.

14. Hence, every cyber defender, user and organisation should understand how human thought and behaviour applies to cybersecurity. In addition, by applying psychological principles, such as inculcating positive social norms, everyone can build safer and more secure ecosystems in cyberspace.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

. . . . .

REFERENCES

1. Cyberpsychology - British Psychological Society
https://www.bps.org.uk/member-networks/cyberpsychology-section

2. 10 Types of Social Engineering Attacks and How To Prevent Them
https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/types-of-social-engineering-attacks/

3. 15 Types of Social Engineering Attacks
https://www.sentinelone.com/cybersecurity-101/threat-intelligence/types-of-social-engineering-attacks/

4. IBM Cost of a Data Breach Report 2024
https://www.ibm.com/reports/data-breach

5. ISACA State of Cybersecurity 2022 Report
https://www.isaca.org/resources/reports/state-of-cybersecurity-2022

6. Why Psychology Matters to Cybersecurity
https://www.infosecurityeurope.com/en-gb/blog/future-thinking/why-psychology-matters-in-cybersecurity.html

7. Hacking the Mind: Why Psychology Matters to Cybersecurity
https://www.ibm.com/think/insights/hacking-the-mind-why-psychology-matters-to-cybersecurity

8. Why Cyberpsychology Is Such an Important Part of Effective Cybersecurity
https://www.csoonline.com/article/643967/why-cyberpsychology-is-such-an-important-part-of-effective-cybersecurity.html

9. Verizon 2023 Data Breach Investigations Report
https://www.verizon.com/business/resources/T6c/reports/2023-data-breach-investigations-report-dbir.pdf

10. Change Blindness - Cysec4psych
https://cysec4psych.eu/psych-cyber-concept/change-blindness/

11. How Do We Truly Make Security ‘Everyone's Responsibility’?
https://www.darkreading.com/cybersecurity-operations/how-do-we-truly-make-security-everyone-s-responsibility