TUS
Technological University of the Shannon: Midlands Midwest
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre Iarthar Láir

TUS Research

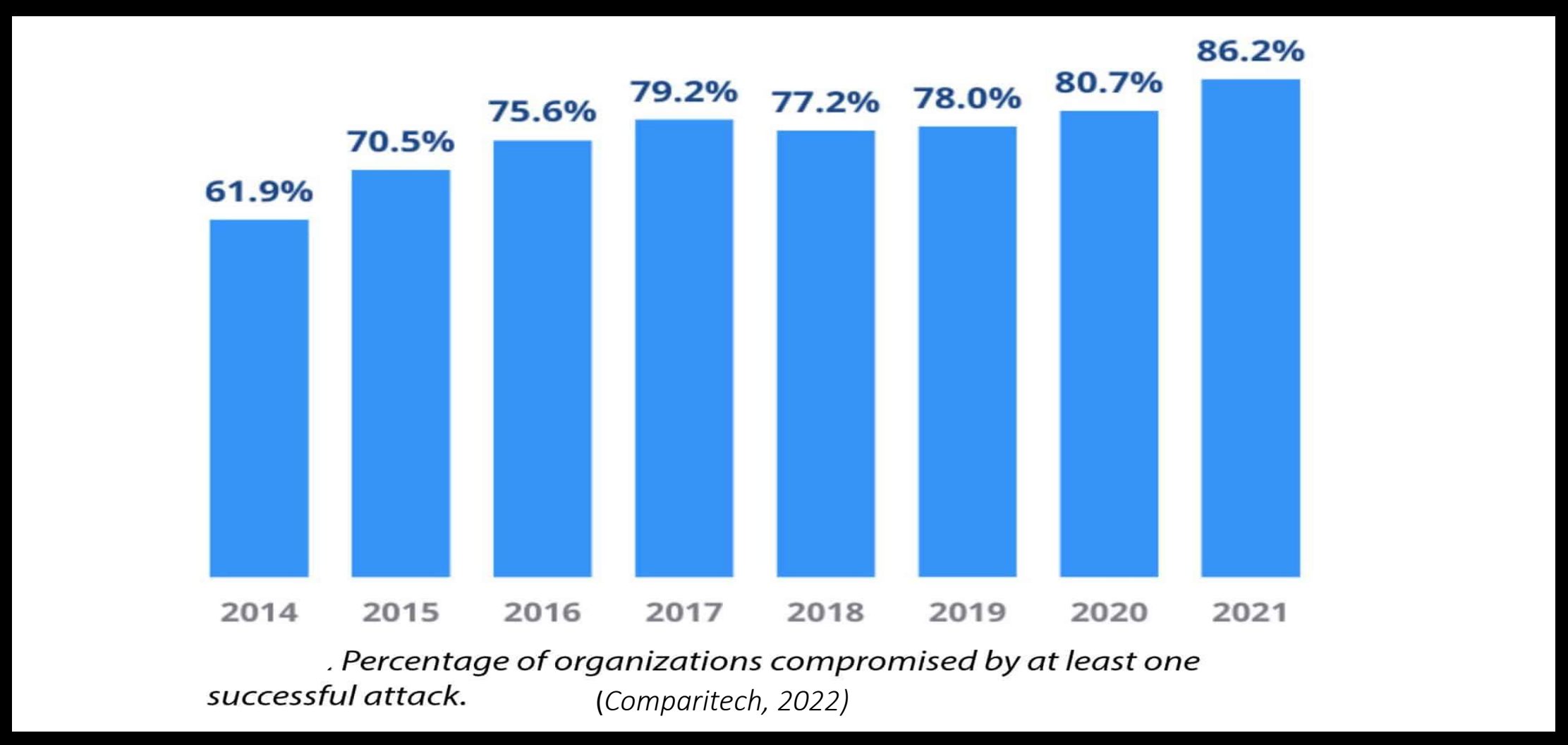
Investigating the Development of Employee Behaviour and Training Towards Cyber-Security in The Irish Credit Unions

Research Overview

The remarkable technology development along with the emergence of mobile applications complexity has increased the number of cyber-attacks in several industries which resulted in serious risks in today's society and cyberspace. To safeguard sensitive data, organisations are investing more than ever before in security systems such as information leak prevention, password management, and computer security monitoring technologies. These tools provide technical support to the cyber-security issue but are not enough to provide total security. One of the primary factors that can either minimize or increase cyber-attacks is the human factor within the organisation. Some employees are simply not aware of the seriousness of cyber threats or decide not to comply with their organisation's information security policy. This project will try to investigate the level of training that employees within the Irish Credit Unions get when dealing with cyber-attacks and try to determine whether employees as well as managers in the Irish Credit Unions are familiar with the technological infrastructures and the risk assessment plan in the organisation. This research will determine the factors affecting employees' psychology towards information security policy compliance in the Irish Credit Unions. This research will also identify areas of concern, ways to eliminate cyber-attacks with view to producing an excellence in employee cyber-security training for the staff of the Irish Credit Unions

Why Cyber-Security?

One of the critical challenges facing the business world today is cyber-attacks. Irish businesses are at high risks of losing their data, finances, and reputation in the market due to such attacks. The Irish economy has lost over €9.6 billion in 2020 on cyber-attacks, this is a huge number showing the seriousness of this phenomena (Goodbody, 2021). The combination of remote working, new technology adoption, the introduction of the 5G, weaker control, and lack of information security training has allowed more routes for cyber criminals to access sensitive data and people's finances. In the financial sector, the threats are even higher with over 30% of the world population using online banking. A survey conducted by Fraud professionals discovered that over 75% of online users have experience fraud in 2020 (ACFE, 2020). Cyber incidents usually involve humans, where employees are not aware of the seriousness of these threats. Technology along with training can indeed enhance employees' awareness towards cyber-security.



. Percentage of organizations compromised by at least one successful attack. (Comparitech, 2022)

AWARENESS
Protect yourself.

The Frontline of Cyber Security!

Research Objectives

The objectives of this research will be to:

- Determine factors affecting employee trust and commitment in the Irish Financial Sector
- Investigate Cyber-Security risk assessment levels within the Irish Financial Sector
- Investigate the level of trust that an employee encounter when faced with the organisational and technical infrastructure at the Irish Financial Institutions
- Evaluate employees' skills and experiences of dealing with cyber threats
- Investigate to what extend employees within the financial institutions are sufficiently trained and aware of the cybercrime threats
- Examine technology usage and adoption in the Irish Credit Unions

Impactful Cyber-Security Facts and Stats / Research Motivation

- 95% of cyber-security breaches are caused by human error (Cybint, 2020).
- A cyber-attack happens every 39 seconds (Gartner, 2020).
- Cybercrimes increased by 300% since the start of the COVID19 pandemic (CBS News, 2021).
- Online Payment fraud will cause the ecommerce sector $25 billion annually by 2024
- More than 77% of organizations do not have an incident response plan
- Remote employees will remain to be a target for hackers (Gartner, 2020).
- The cyber-security skills lack will continue to be a problem (Proofpoint, 2020).
- With the introduction of the 5G, IoT devices will become more vulnerable to cyberattacks (Verizon, 2020).
- 68% of business leaders feel their cyber-security risks are increasing (Verizon, 2020).
- An estimated 300 billion passwords are used by humans and machines worldwide (Cybint, 2020).
- Phishing attacks account for more than 80% of reported security incidents (ACFE, 2020).
- On average, every employee has access to 11 million files (Cybint, 2020).

References

ACFE. (2020). *FRAUD IN THE WAKE OF COVID 19: BENCHMARKING REPORT.*

- Patterson, D. (2021, May 19). *Cybercrime is Thriving during the pandemic, driven by surge in phishing and ransomware. CBS News*
- Devon. (2020, December 23). *15 Alarming Cyber Security Facts and Stats.* Cybintsolutions.
- Proofpoint. (2020). *State of the Phish, An in-depth look at user awareness, vulnerability and resilience: Annual Report.*
- Garner. (2019, November 19*). Cloud Shift Impacts All IT Market*. Garner.
- Goodbody, W. (2021, November 23). Cybercrime cost Irish economy €9.6bn last year. *RTE*
- Verizon. (2020). *2020 Data Breach Investigations Report.*

Acknowledgment

This research has received funding from the presidential seed grant program offered by TUS and is supported by Athlone's Credit Unions

This project is supervised by:
Dr. Aisling Keenan "Faculty of Business and Hospitality"
Dr. Brian Lee "Director of Software Research Institute TUS"

Financial Services Ireland
Ibec

Credit Union

CYBER|IRELAND
IRELAND'S CYBER SECURITY CLUSTER

NATIONAL CYBER SECURITY CENTRE
NCSC

Mr. Reda Jouaibi

Email:
A00277271@student.ait.ie

TUS
Technological University of the Shannon: Midlands Midwest
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre Iarthar Láir

TUS Research