Evaluasi Tingkat Kesadaran Keamanan Informasi: studi kasus Sekretariat Utama Badan XYZ = Information Security Awareness Evaluation: Case Study Principal Secretariat of the XYZ Agency

Canny Siska Georgina, author

Abstrak

Dalam keamanan informasi, aspek paling kompleks seperti sosioteknis dan faktor manusia, masih menjadi “rantai terlemah” dan paling sulit dipahami dalam menciptakan lingkungan digital yang aman. Sehingga, evaluasi kesadaran keamanan perlu dilakukan berkala untuk memastikan bahwa seluruh anggota Settama Badan XYZ, yang setiap harinya memiliki tugas dan tanggung jawab terhadap pengelolaan data strategis organisasi, dapat memahami risiko keamanan hingga konsekuensi dari perilaku/tindakan yang dilakukan di pekerjaan. Tujuan penelitian ini adalah untuk mengevaluasi kesadaran keamanan informasi personel Settama Badan XYZ. Penelitian dilakukan dengan pendekatan kuantitatif melalui kuesioner dan eksperimen melalui simulasi phishing. Kuesioner yang digunakan mengadopsi framework Knowledge, Attitude, dan Behavior (KAB), yang dikombinasikan dengan Human Aspects of Information Security Questionnaire (HAIS-Q), Indeks KAMI, dan masukan pakar dengan total 81 pertanyaan. Sedangkan untuk pendekatan eksperimen menggunakan framework dan simulator Gophish. Sampel penelitian adalah pegawai Settama Badan XYZ yang dipilih secara acak, dengan jumlah 200 orang untuk pengisian kuesioner dan 100 orang untuk simulasi phishing. Sebelum dilakukan perhitungan skor akhir, dilakukan kalkulasi pembobotan prioritas dengan pendekatan analytic hierarchy process (AHP), untuk setiap fokus dan subfokus area yang diteliti. Skor akhir kesadaran keamanan informasi pegawai Sekretariat Utama adalah 83,74%, dan dapat dikategorikan baik berdasarkan skala Kruger. Namun, masih terdapat dua fokus area yang berada dalam kategori menengah, yaitu penggunaan internet (77,73%) dan komputasi seluler (76,21%), serta satu subfokus area yaitu mengklik tautan e-mail dari pengirim yang dikenal (62,04%). Di sisi lain, hasil simulasi phishing menunjukkan success rate yang cukup tinggi untuk kedua skenario simulasi. Pada skenario simulasi pertama, diantara 30 pegawai yang membuka e-mail, 100% pegawai (30 orang) mengklik link umpan ke landing page decoy, dan 80% pegawai (24 orang) mengisikan kredensial mereka disana. Sedangkan pada skenario kedua, masih ditemukan 95,5% pegawai (21 orang) diantara 22 pegawai yang membuka e-mail, mengklik link umpan ke landing page decoy, dan 45,5% pegawai (10 orang) memasukkan kredensial mereka. Perbedaan pada hasil kuesioner dan hasil simulasi menunjukkan bahwa masih terdapat gap antara pengetahuan, sikap, dan perilaku pegawai Settama Badan XYZ. Terlihat bahwa pegawai sebenarnya telah memiliki pondasi pengetahuan dan pemahaman yang baik terkait cybersecurity/information security awareness, namun belum benar-benar termanifestasi dalam bentuk tindakan/perilaku saat di pekerjaan.

..... In information security, the most complex aspects, such as sociotechnical and human factors, are still the “weakest link” and most difficult to understand when creating a secure digital environment. Thus, security awareness evaluations need to be carried out periodically to ensure that all personnels of the Principal Secretariat of XYZ Agency, who have duties and responsibilities for managing the organization's strategic data every day, could understand security risks and the consequences of behavior/actions established inherently at work. Therefore, the purpose of this research is to evaluate the information security

awareness of The Principal Secretariat's personnel. The study was carried out using a quantitative and experimental-based approach through questionnaires and phishing simulations, respectively. Our questionnaire used the Knowledge, Attitude and Behavior (KAB) framework, which was then combined with the Human Aspects of Information Security Questionnaire (HAIS-Q), the KAMI Index, and expert's input with a total of 81 questions. At the same time, the experimental approach used the open-source Gophish framework and simulator. The research sample was XYZ agency's Principal Secretariat employees who were randomly selected, with 200 personnels to fill out the questionnaire and 100 personnels for the phishing simulation. Before calculating the final score, priority weighting calculations were first carried out using the analytic hierarchy process (AHP) approach, for each focus and sub-focus area used in this study. The final score for information security awareness of Principal Secretariat's employees is then calculated using a simple scorecard method, resulted in 83.74%, thus can be categorized as good based on the Kruger scale. However, there are still two focus areas classified in the middle category, namely internet use (77.73%) and mobile computing (76.21%), as well as one sub-focus area, namely clicking on e-mail links from known senders (62, 04%). On the other hand, the phishing simulation results show a fairly high success rate for both scenarios. In the first simulation scenario, among 30 employees who opened e-mail, 100% of employees (30 personnels) clicked on the false link to the decoy landing page, and 80% of employees (24 personnels) actually filled in their credentials. Meanwhile, in the second scenario, it was still found that 95.5% of employees (21 personnels) among 22 employees who opened the e-mail, clicked on the fake link to the decoy landing page, and 45.5% of employees (10 personnels) still entered their credentials. The difference between the results of the questionnaire and the simulation shows that there is still a gap between the knowledge, attitudes and actual behavior of XYZ agency's Principal Secretariat employees. It is shown that employees can in fact, have sufficient amount of knowledge and understanding regarding cybersecurity/information security awareness, but at the same time, couldn't apply those knowledge in the form of actions during work.