BAB V

PENUTUP

5.1. Kesimpulan

Berdasarkan tahapan penelitian yang telah dilakukan dari tahap awal hingga akhir, terdapat beberapa poin yang dapat disimpulkan antara lain sebagai berikut:

1. Tingkat kesadaran karyawan terhadap *phishing* email secara umum rendah, ditunjukkan dengan 47 karyawan membuka email, 32 karyawan mengklik *link* pada *email,* 4 karyawan memasukan data sensitif berupa email & *password*, dan hanya 7 karyawan yang melaporkan terdapat *phishing email*.
2. Dalam konteks ISO/IEC 27001:2022, penerapan simulasi *phishing* email ini selaras dengan kontrol dalam Annex A.6.3 "*Information security awareness, education and training*", di mana organisasi diwajibkan untuk memastikan seluruh personel mendapatkan pelatihan dan peningkatan kesadaran terhadap keamanan informasi. Pelatihan ini harus mencakup berbagai ancaman keamanan siber, termasuk *phishing*, serta dilakukan secara berkala dan diperbarui sesuai perkembangan ancaman. Penelitian ini menunjukkan bahwa *awareness* yang dilakukan dan simulasi *phishing* merupakan salah satu bentuk nyata implementasi kontrol tersebut.
3. Dalam konteks PCI DSS v4.0, khususnya pada *requirement* 12.6.3.1, organisasi diwajibkan memberikan pelatihan kesadaran keamanan yang mencakup ancaman *phishing* dan serangan *social engineering.* Simulasi *phishing* yang dilakukan dalam penelitian ini merupakan salah satu bentuk implementasi dari kontrol tersebut. Berdasarkan hasil simulasi dan wawancara, perusahaan telah mengadopsi praktik baik yang di haruskan dalam PCI DSS seperti:
    a. Menyediakan *awareness training* tentang *information security & phishing* bagi karyawan, dibuktikan dengan terlaksana nya *awareness* dan *phishing attack simulation*.

b. Memberikan panduan bagaimana mengenali dan merespons *phishing*, dibuktikan dengan terdapat panduan pada information security awareness, terdapat *channel* untuk pelaporan insiden phishing, dan panduan di dalam ISMS Policy seperti pada Lampiran 6.
c. Mendorong pelaporan insiden mencurigakan ke tim internal, dibuktikan dengan adanya karyawan yang melaporkan adanya *phishing email* kepada tim internal

5.2. Saran

Berdasarkan penelitian yang telah dilakukan, terdapat beberapa saran untuk penelitian selanjutnya yaitu sebagai berikut:

1. Melakukan pada lebih dari satu perusahaan, khususnya dengan tingkat keamanan informasi yang berbeda, baik yang sudah tersertifikasi ISO 27001 dan/atau PCI DSS maupun yang belum.
2. Menggunakan skema simulasi *phishing* secara berkala dan bervariasi, misalnya dengan jenis email yang berbeda (*invoice*, hadiah, *impersonation* atasan) untuk menguji daya tanggap karyawan secara lebih menyeluruh.
3. Melakukan serangan *phishing email* dengan berbagai kategori, kategori berdasarkan usia, jenis kelamin, atau latar belakang pendidikan.
4. Perusahaan disarankan untuk menyelenggarakan pelatihan keamanan informasi secara berkala dengan pendekatan yang lebih interaktif, seperti *microlearning*, video simulasi, atau kuis interaktif.