O capital humano é a melhor defesa contra ciberataques

Um artigo traduzido pela Acumen

2022

ACUMEN

seniormanagementworldwide
leading global provider of interim executives

As seis estratégias definidas neste artigo são recomendadas para fortificar a "*firewall* humana" contra as técnicas fraudulentas de *hackers,* e fomentar uma cultura organizacional consciente em termos de cibersegurança.

As seis recomendações seguintes são uma forma estratégica e rentável para os líderes combaterem os riscos de segurança relacionados com a informação, através da psicologia humana.

1. Defina uma política de segurança para a empresa

Com a criação de um código de ética, torna os colaboradores mais comprometidos, mais propensos a seguir normas e a uma maior adesão cognitiva e comportamental com os códigos de conduta. Estas políticas são compromissos escritos que declaram que um colaborador, por exemplo, tratará com confidencialidade todas as informações da empresa (por exemplo, dados de clientes), procederá de acordo com o melhor interesse da organização durante as suas atividades online e offline, e reporta incidentes suspeitos imediatamente para o respetivo ponto de contacto interno. Os colaboradores também reconhecem que não divulgarão nenhuma informação sensível da empresa a quaisquer partes externas.

Por exemplo, a CISCO exige que os seus colaboradores assinem anualmente um código de conduta empresarial que define como proteger a propriedade intelectual da empresa, bem como os ativos de informação confidenciais. A empresa exige que os seus colaboradores não partilhem informações confidenciais com entidades que não tenham necessidades comerciais legítimas. Uma cultura corporativa que repreenda os erros pode desencorajar os colaboradores a relatar atividades suspeitas, mas ao pedir aos colaboradores que assinem uma política que sinalize a sua responsabilidade em reportar atividades suspeitas poderá resolver esta questão.

2. Liderar pelo exemplo

Em cenários de incerteza, as pessoas procuram estratégias sobre como pensar e agir. Por um lado, este comportamento pode ser enquadrado como atuar em conformidade, mas por outro, pode ser visto como uma forma de ajudar as pessoas a entender uma compreensão comum do comportamento correto ou normativo.

Procurar outras estratégias ajuda a reduzir a incerteza - especialmente quando as estratégias adotadas vêm de pessoas com posições sociais respeitadas. A chefia deve, portanto, dar o exemplo e promover boas práticas.

As empresas devem, por exemplo, enfatizar a importância de comportamentos em prol da segurança, como não deixar o seu computador pessoal desbloqueado, não abrir websites no computador da empresa sem verificar a sua legitimidade, e não expor documentos da empresa, sejam eles físicos ou digitais, em espaços públicos. Recomendamos que os líderes também forneçam exemplos de incidentes de violação de cibersegurança em que foram descuidados ou onde foram relatados comportamentos descuidados. Fazê-lo ajudará a reduzir a sensação de vulnerabilidade entre os colaboradores.

3. Cultivar a reciprocidade

Existe uma norma social generalizada que dita que se alguém nos oferecer algo, nós sentimo-nos obrigados a retribuir o favor. Este impulso tende a ser verdadeiro mesmo que a oferta original não tenha sido solicitada ou mesmo se o que é solicitado em troca seja muito mais valioso do que o que foi inicialmente dado. A norma da reciprocidade é importante, porque muitas vezes o favor devolvido é feito

de forma inconsciente.

Os líderes devem estar cientes desta poderosa técnica para influenciar os colaboradores, e usá-la para fortalecer uma cultura consciente da segurança na organização. Tomar medidas para garantir os dados ou identidade de um colaborador, como fornecer-lhes *flash drives* seguras e encriptadas, ou com uma moldura digital personalizável que exibe lembretes de segurança pode ser um passo significativo para provocar reciprocidade.

4. Aumentar o interesse dos colaboradores em cibersegurança

As pessoas percebem objetos e oportunidades de forma mais atrativa se forem raros, escassos ou difíceis de obter. As empresas podem recorrer a esta tendência psicológica para promover acreditações de cibersegurança raras e exemplares na organização, tais como processos de segurança da informação acreditados, que podem ser comprometidos por uma falha de segurança.

Ao comunicar abertamente com os colaboradores, os executivos reforçarão o compromisso dos colaboradores com uma cultura de segurança. Além disso, a administração deve promover a criação de um sistema de classificação que qualifique a informação sensível em diferentes níveis. Os colaboradores irão adquirir um sentido para a escassa informação que os mantém atentos na proteção ativa da informação confidencial da empresa, em vez da tarefa ilusória de proteger toda a informação, independentemente da sua criticidade.

5. Liderar pelo exemplo

As pessoas são mais influenciadas por quem se identificam e gostam, e os líderes podem ganhar a confiança dos colaboradores ao interagir com humildade e empatia. Os líderes que mostram vulnerabilidade são suscetíveis de receber empatia e simpatia em troca. Esta reciprocidade pode promover indiretamente o cumprimento dos dirigentes em termos de comportamentos de segurança ideal. Partilhar os seus erros relacionados com cibersegurança e a forma como aprendeu com estes erros aumenta a probabilidade de os colaboradores seguirem o seu exemplo.

6. Alavancar o valor da autoridade

Normalmente, as organizações exigem que os seus colaboradores façam uma formação anual em cibersegurança. Quando a administração, que os colaboradores vêm como a autoridade organizacional, instruir pessoalmente os seus trabalhadores a cumprirem os requisitos de segurança da informação corporativa, serão mais propensos a obter os resultados desejados. Mas há um problema: os líderes precisam de ser vistos como uma fonte de confiança, além de serem apenas vistos como uma entidade hierarquicamente superior. É a diferença entre apenas ser autoritário, e ordenar à força de trabalho o que fazer, e ser visto como "uma autoridade", detentora de conhecimentos. Possuir ambos é a combinação mais eficaz.