NÍVEIS DE MATURIDADE EM PROGRAMAS DE CONSCIENTIZAÇÃO

Você certamente sabe que existem diversos modelos de maturidade que possibilitam com que as empresas identifiquem o nível de capacidade para evoluir e/ou executar um projeto, não é mesmo? Pois saiba que, em 2011, o SANS Institute contou com a participação de mais de 200 especialistas em conscientização de segurança cibernética para criar o Modelo de Maturidade de Conscientização em Segurança, que rapidamente se transformou em um verdadeiro padrão para a indústria.

COMO ELE FUNCIONA?

O Modelo SANS de Maturidade de Conscientização em Segurança é composto por cinco níveis que identificam o nível de maturidade de um programa de conscientização dentro de uma companhia. Ele pode ser utilizado como um roadmap por corporações que desejam aprimorar (ou até mesmo implementar um do zero, caso ainda não tenha) o seu programa de conscientização, listando indicadores, tempo estimado para atingir cada um dos níveis e métricas que você deve utilizar. Neste conteúdo, vamos nos aprofundar um pouco mais sobre esse modelo e como ele pode ser útil para transformar seus colaboradores na linha de frente de sua estratégia de defesa cibernética!

1° NÍVEL
NÃO-EXISTENTE

O nome diz tudo: neste nível, a empresa não possui um programa de conscientização, os colaboradores não fazem ideia das ameaças às quais eles estão expostos e nem possuem conhecimento sobre segurança.

As lideranças não falam sobre o assunto, não há métricas e a corporação corre perigo por estar vulnerável a incidentes. O primeiro passo para sair dessa estagnação é identificar padrões e regulamentos setoriais, escolher o executivo responsável pelas ações de conscientização e iniciar o desenvolvimento do programa. Infelizmente, ainda existem empresas que se encontram neste primeiro nível.

2° NÍVEL
FOCO EM COMPLIANCE

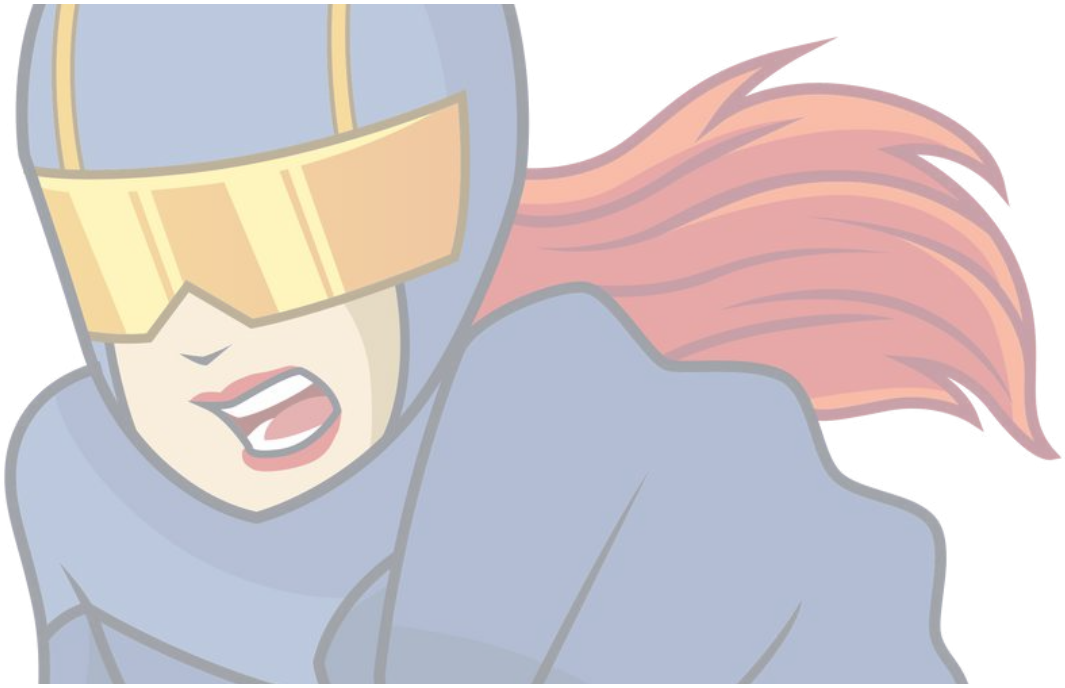
O programa existe, mas ele é resumido em ações pontuais (como boletins mensais e palestras anuais) com o único objetivo de garantir conformidade com as normas regulatórias de seu setor; nada mais.

Neste nível, os colaboradores continuam incertos sobre as políticas de privacidade da empresa, enxergam cibersegurança como uma obrigação chata e possuem uma percepção negativa do tema. Não há um plano estratégico e o suporte da diretoria é quase nulo, já que o objetivo é gastar o mínimo possível. As métricas são simples, como o cálculo da porcentagem de quantas pessoas completaram determinada atividade.

3° NÍVEL
PROMOÇÃO DE CONSCIÊNCIA E MUDANÇA DE HÁBITOS

Este é o estágio que você deve almejar: aqui, sim, o programa é devidamente elaborado para engajar os colaboradores e promover uma mudança cultural profunda em seus hábitos cotidianos. Como resultado, as equipes passam a entender seu papel na segurança de dados corporativos, entendem as políticas internas e são capazes de reconhecer e reportar ameaças.

Este nível também demanda uma colaboração maior das lideranças, um plano estratégico com um escopo e objetivos bem-definidos e métricas mais específicas, como estatísticas de simulações de phishing, dispositivos infectados por mês, quantidade de políticas violadas e assim por diante. Estima-se que uma empresa pode atingir tal nível com um esforço de três a seis meses.



4° NÍVEL
SUSTENTAÇÃO A LONGO PRAZO E MUDANÇA CULTURAL

Poucas empresas conseguem chegar aqui. Porém, aquelas que conseguem usufruem de um programa de conscientização robusto, com alto apoio da diretoria e planejado para ter um longo ciclo de vida, incluindo, no mínimo, uma revisão anual para adequá-lo às novas ameaças e riscos cibernéticos.

A mudança cultural em seus colaboradores é tão grande que eles passam a integrar segurança em tudo o que fazem, educando outras pessoas sobre práticas seguras e participando ativamente de todas as iniciativas de proteção de dados sensíveis. Como métricas, podemos estudar as atitudes e percepções dos colaboradores sobre segurança da informação, além de analisar o número de pessoas ou departamentos requisitando novas informações e dando sugestões sobre as estratégias corporativas de segurança. Chegar em tal estágio demanda de três a dez anos de muito esforço, com analistas focados em tempo integral em seu programa de conscientização.

5° NÍVEL
MÉTRICAS ROBUSTAS

Não se engane: métricas são importantes em todos os estágios de maturidade de seu programa de conscientização. Porém, neste último nível, as ações possuem métricas tão robustas e alinhadas com a missão da companhia que elas de fato se tornam essenciais para o aprimoramento contínuo do programa e para demonstrar o retorno sobre o investimento (ROI).

Número de incidentes, tempo necessário para identificar e se recuperar de um incidente... Esses são só alguns exemplos de estatísticas que podem ser concentradas em um dashboard de fácil visualização, facilitando o encontro de eventuais lacunas e criação de relatórios (sejam eles para uso interno ou externo). Podemos concluir que as métricas, na verdade, são necessárias para a sustentação a longo prazo, já que é a partir delas que é possível mensurar o impacto causado pela cultura de cibersegurança na empresa.

Não é fácil atingir os níveis mais altos do Modelo SANS de Maturidade de Segurança. Porém, com uma plataforma de gamificação como a Hacker Rangers, a tarefa de engajar os colaboradores com conteúdos de qualidade e sempre atualizados se torna bem mais simples. Conheça a plataforma agora mesmo e não fique estagnado no nível mais básico de conscientização!

HACK3R_
RANGER5

Bibliografia
SANS Maturity Model (SANS Institute, agosto de 2021)
Security Awareness Maturity Model - Part 1 (Haekka, dezembro de 2020)

TESTE A NOSSA PLATAFORMA GRATUITAMENTE DURANTE 15 DIAS!
HACKERRANGERS.COM.BR