KnowBe4

お金のデザイン THEO [テオ]

CASE STUDY

煙たがられがちなセキュリティ研修や訓練を楽しみな時間に変え、リテラシーを向上

安全を担保し、かといってガチガチに縛り付けない落とし所を模索

世の中、お金に関する不安は尽きることがない。そんな中お金のデザインでは、一人ひとりにあった資産運用を提案するロボアドバイザー「THEO [テオ]」など、金融工学とテクノロジーを駆使した金融サービスを提供している。
FinTech企業として、より便利で価値の高いサービスを顧客に安心して使ってもらうには、セキュリティ対策やITガバナンスが不可欠だ。同社のコンプライアンス部ITガバナンスグループ長、水谷義和氏は「業務やサービスに支障を来すほどガチガチにしすぎることなく、しかし必要なセキュリティを担保するため、常に最適なバランスを探りながら対策に取り組んでいます」という。リスクアセスメントを行い、弱い部分があればリスクの大きさやコストと照らし合わせて対応策を検討していく王道のアプローチに基づいて対策を進めてきた。

ヒューマンファイアウォールの構築は不可欠だが、負荷の増大が課題に

そんな対策の一つが従業員に対するセキュリティ教育だ。「アンチウイルスソフトなどのセキュリティ対策製品を導入していますが、人間は意図せず悪意あるものを招き入れてしまうこともあるため、それだけでは守れないことは確実です。従業員のITリテラシーを高め、ヒューマンファイアウォールの構築が非常に大事だと常に考えています」（水谷氏）
新たに社員が入社した際にはセキュリティも含めたIT全般について研修を行い、一定水準のITリテラシーを持って業務に当たってもらうことを前提にしてきた。さらに定期的に情報セキュリティ研修を行うほか、実際の攻撃に模した訓練メールを送付して見破り方、およびその後の対応について身をもって学ぶ標的型攻撃メール訓練も実施し、常にレベルアップを図ってきた。
しかし、そのために水谷氏にかかる負荷は大きかった。「今のように生成AIが登場する以前は、攻撃者の視点に立って、一から訓練メールを作成していました。その時々の状況、最新の脅威トレンドを考慮し、あれこれ考えながら自力で作成していましたが、次第にアイデアが枯渇してきたことに加え、多くの時間が取られていました」（水谷氏）
標的型攻撃メール訓練は実施しただけでは意味がない。結果をまとめて報告し、また従業員にはフィードバックやフォローを行うことではじめて意義あるものになる。だが、四半期ごとに行われる研修や訓練の準備からまとめまでのサイクルを一度回すだけで2～3ヶ月はかかり、「ずっと研修や訓練関連の業務に追われる状況でした」（水谷氏）
また、それ以前に採用していた海外製eラーニングの教材はコンテンツの種類が少ない上に、日本語の翻訳の質にも課題があった。加えて、理解度を確認する手段も用意されていなかったため、「結局、自分で簡単な確認テストを作成する手間もかかっていました」（水谷氏）

株式会社お金のデザイン

業界

金融

本社

東京都千代田区

キーフレーズ

「セキュリティの研修を楽しみ、『次も見たい』と言ってもらえるのは、奇跡的なことではないかと思います」

株式会社お金のデザイン
コンプライアンス部
ITガバナンスグループ
ITガバナンスグループ長
水谷義和氏

ポイント

- 豊富なテンプレートを生かして労力を減らしつつ、訓練メールのヒット率の減少と通報増加を実現
- 従業員が楽しめる研修動画を通してセキュリティの知識を吸収し、リテラシーを向上

訓練だけに終わらせず、平時の業務もカバーできる点を評価

そんな同社は以前から、ITシステムやセキュリティに関する悩みをサイバネットシステムに相談していた。「僕の中では第一窓口はサイバネットシステムです。世間話からセキュリティ課題まで、ざっくばらんに様々な相談に乗っていただいていました」（水谷氏）
コンテンツの質や量、負荷といったセキュリティ教育に関する悩みを口にしたところ提案されたのが、KnowBe4の「KSAT」と「PhishER」だった。
国産のセキュリティ教育ソリューションも含め、他にもいくつか選択肢があったのは事実だ。だが水谷氏には、日本語も含めて多言語に対応し、豊富なコンテンツとテンプレートが用意されていることに加え、選定に当たって譲れないポイントがあった。不審メールを受け取ったときにITガバナンスグループに報告する「通報ボタン」が、訓練だけでなく通常時でも利用できることだ。「訓練は年に何日かしかありません。KSATの通報ボタンは、訓練時にしか使えないのではなく、平時の通常業務中においても従業員に届いた本物の不審メールも通報できる点を評価しました」
（水谷氏）
加えて、KSATと同時に導入したEmail SOAR製品であるPhishERに含まれる複数のウイルス対策スキャナを利用して悪意あるコンテンツが含まれていないかどうかをチェックするサービス「VirusTotal」で、危険なものかそうでないかを自動的に検査できる点も魅力だった。「担当が私一人しかおらず、やるべきことが他にも多々ある中で、KnowBe4製品に一任できる部分が多いため、非常にありがたい存在です。もはや相棒と言ってもいいかもしれません」と水谷氏は評価する。
海外製のソリューションにつきものの翻訳の品質やサポート面での不安がないわけではなかったが、「サイバネットの提案でトライアルを実施してみたところ非常に使いやすく、すんなり導入できました。いい意味で『別物』でした」（水谷氏）と振り返った。

繰り返しの訓練と研修でセキュリティリテラシー向上に確かな手応え

お金のデザインでは2024年3月にKnowBe4のKSATおよびPhishERを導入し、セキュリティ研修と標的型攻撃メール訓練をそれぞれ年に4回実施している。双方を3ヶ月に一回というペースで実施していることになるが、KSATに付属している充実した訓練メールテンプレートを活用することで、手作りしていた頃に比べると作業負荷は大幅に軽減された。「体感では工数が5〜6割は減っています」（水谷氏）
また、訓練で疑似メールに引っかかってしまった対象者をリスト化し、リマインドを送信してフォローアップのための研修を受講させるまでのプロセスも自動化できる点もポイントだ。「誤ってメールを開いてしまった人たちをそのままにしておくと会社のリスクになりかねません。その人たちを絶対に逃がさないぞという意気込みでフォローアップしていたのですが、そこも僕が都度手作業で抽出し、対応する必要がなくなりました。相棒様々です」（水谷氏）
こうした取り組みを繰り返すことで、従業員のセキュリティリテラシー向上についても確かな手応えを感じている。
以前は、誤って引っ掛かってしまう割合が三割程度あった上に、そのことを通報しない従業員も少なくなかった。しかし「訓練の回数をこなすにつれてヒット率は減少し、業界全体のベンチマークを大きく下回る一桁台にまで下がっています。また、訓練時はもちろん、通常業務における不審メールの通報自体も増えてきました」と水谷氏は実績を評価した。

たとえ「自分は大丈夫」でも、他の同僚が引っかかってしまえば組織全体がリスクにさらされてしまう。水谷氏はそんな事態を防ぐため、通報のやり方を実践してもらうための独自の訓練を企画・実施し「全社通知につなげるため、まずは一報を」と呼び掛けてきた。その成果が確実に実りつつあり、「Slackで『こんな不審なメールがあったので通報しておいたよ』とメッセージをもらうこともあります」という。通報が寄せられ、悪意あるものと判定されたメールを他の従業員のメールボックスから自動的に探して消去させるPhishERの「隔離」機能のメリットも感じているという。
一方、研修ではKnowBe4の提供する動画の中から、その時々の状況や課題に合わせて数本をピックアップし、組み合わせて閲覧してもらっている。
「いくつか海外ドラマ調のコンテンツがありますが、従業員からは、ただ勉強になるだけでなく楽しめると非常に好評です。セキュリティというものは、従業員からすると『何でこんなことをしなければいけないの』と煙たがられがちですが、KnowBe4の動画は見やすく、面白いため、するすると吸収できます。セキュリティの研修を楽しみ、『次も見たい』と言ってもらえるのは、奇跡的なことではないかと思います」（水谷氏）

検討から導入、運用に至るまでのサポートにも満足している。「KnowBe4はコンテンツが非常に豊富であるがゆえに、目的に合致したものを探すのが大変なこともありますが、『こんな目的でこんな内容のものを探しています』とKnowBe4のカスタマーサクセスマネージャーに伝えると、すぐにぴったりのコンテンツや、それを探すための検索キーワードを教えていただけました」（水谷氏）と的確な支援を評価している。

生成 AI の活用も視野に、さまざまな形で対策強化を継続

お金のデザインは今後も、技術の進化や脅威の変化に合わせて対策を強化していく方針だ。特に注目しているのは、やはり生成AIだという。「従前の対策に加え、これからのセキュリティ対策にはAIは欠かせない存在になってくると考え、共存していきたいと思っています」（水谷氏）
脅威検知系のシステムでの活用はもちろんだが、「KnowBe4でも、従業員一人一人のリスクスコアに基づいてトレーニングをパーソナライズするAIDAのようにAIが活用され始めています。標的型メール訓練以外にも、さまざまなシーンでの活用を検討していきたいと思います」（水谷氏）

© 2025 KnowBe4, Inc. All rights reserved.Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.