脆弱性として悪用可能な人間の特性

セキュリティにおける人的要因

「鎖の強さは最も弱いつなぎ目で決まる」という格言がありますが、情報セキュリティの場合、最も弱いつなぎ目に当たるのは人的要因です。すべての事業体において、高レベルのリスク要因は従業員です。[1] Verizon の「2020 年データ侵害調査報告書」によれば、成功したサイバー攻撃の 67%は、人間の過失または人間を基盤とした攻撃、例えばフィッシングなどの結果です。[2] 他の統計でも、サイバー攻撃の 98%は、人的要因とソーシャルエンジニアリング技法に基づいているものであることが明らかにされています。[3] このようなデータが明確に示しているのは、人間の脆弱性が攻撃者によって、ターゲットシステムへのアクセス権取得、スピアフィッシング詐欺、マルウェアの拡散、その他の IT システム脆弱性の突破、ソーシャルエンジニアリング技法に悪用されているという事実です。[4]

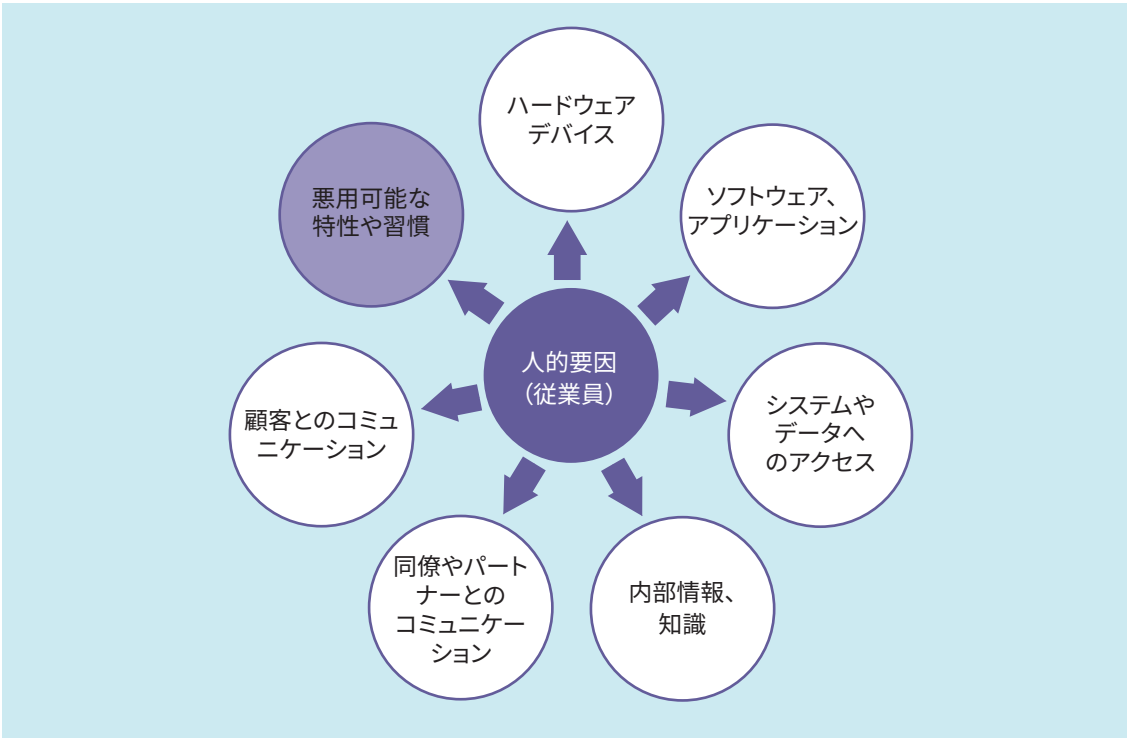
ある文献には、「サイバーセキュリティは、プログラムの問題を超え、むしろ人とプロセスの問題である」と記述されています。[5] 従業員は事業体が保護したいすべての資産に直接アクセスできるため、サイバー攻撃者にとっては使いやすいリソースなのです。従業員は、ハードウェアデバイス（ノート PC、スティックドライブなど）の使用および持ち運び、ソフトウェアのインストールと更新、アプリケーションの実行、重要なファイル、システム、データへのアクセスを行い、有益な内部情報や知識を持ち、同僚、クライアント、パートナーと通信するなど、ソーシャルエンジニアリング攻撃の格好のターゲットとなる悪用可能な特性を有します。[6]

悪用可能な人間の特性、習慣、状況

人は多くの特性や習慣を持ちますが、サイバー攻撃者はそれらを簡単に悪用できます。例えば、面倒見の良さは、ソーシャルエンジニアが手練手管

Eszter Diána Oroszi、CISA、CRISC、CISM
ハンガリーの情報セキュリティコンサルティング企業の主席コンサルタントです。情報セキュリティの分野で12年の実績を有し、人間を基盤とする攻撃、ソーシャルエンジニアリング監査、セキュリティ意識向上に特に関心を持っています。国立公共サービス大学（ブダペスト、ハンガリー）の博士課程に在籍する大学院生で、ゲーミフィケーションを用いたユーザーのセキュリティ意識レベルの測定とその向上について研究しています。

図表1：従業員と職場資産との関係



を用いて悪用できる最も基本的な人間の特性の１つです。同様に、好奇心、信じやすさ、無邪気さもフィッシング攻撃及びマルウェアの拡散に利用される可能性があります。攻撃者は、ユーザーの注意力散漫、油断もしくは無知を利用する場合もあります。攻撃者は、対象の特性、特徴、行動、スキルもしくは知識を特定・分析し、それを悪用できる状況を生み出すことで、絶好のターゲットを選びます。

「人格的特性とは、ある特徴的なパターンの思考、感情もしくは行動が、関連のある状況において、長期にわたって一貫性を持つ傾向があります」[7] 心理学者や人事部門は、問題解決、スキルの向上や活用、人材の適切なキャリアパスの特定のために人格分析やプロファイリングをよく用います。人格分析にはいくつかの方法があります。

- ゴールドバーグの「ビッグファイブ」モデルでは、人間の特性を5つのグループ（経験に対するExtraversion（外向性）、Agreeableness（協調性）、Conscientiousness（誠実性）、Neuroticism（神経症傾向）及びOpenness（開放性））に分類します（順番を入れ換え、OCEANモデルとも呼ばれます）。[8]
- マーストンのDiSCモデルは、4つのカテゴリ（Dominance（主導）、influence（感化）、Stability（安定）及びConscientiousness（慎重））から構成されます。[9]
- マイヤーズ・ブリッグス・タイプ指標は、外向性もしくは内向性、感覚もしくは直感、思考もしくは感情、及び判断もしくは知覚という二分法を用いて4つのグループを定義し、それらを組み合わせて16種類の人格タイプを特定します。[10]

「攻撃者は、対象の特性、特徴、行動、スキル、知識を特定・分析し、それを悪用できる状況を生み出すことで、絶好のターゲットを選びます」

- Mann法は、4つの人格プロファイル（現実派、感覚派、思考派及び協調派）を定義し、それらを一般的な職場での役割に割り当てます。例えば、経営者は一般的に結果重視（現実派）、研究者や財務畑の従業員はほとんどが安全重視（思考派）、マーケティング部門の従業員は自分重視（感覚派）のことがあり、店員や管理者は関係重視（協調派）です。[11]

Mann 法は、従業員の脆弱性や人的リスク要因を理解する際に役立ちます。攻撃者が各役割の意欲、原動力及び一般的な性格を把握すると、その特性を悪用できます。ただし、従業員が各人格タイプと関連するリスク要因を意識していれば、最も適切なリスク軽減対策を特定し、必要な手順を踏んでセキュリティ意識を向上させることができます。

悪用可能な特性や習慣は、個人、職場、瞬間及び状況という４つの大きなカテゴリに分けることができます（**図表 2**）。[12]

この４つの特性カテゴリは関連付けたり、共有させたりすることができます。そのような組み合わせがソーシャルエンジニアに悪用されるのです。例えば、面倒見が良く、見知らぬ顧客ともよくコミュニケーションを取る新入社員が休暇中の場合、攻撃者はその従業員に電話で連絡を取り、顧客の名を騙って機密情報を聞き出そうとします。その従業員は入社したばかりで、業績評価を上げたい

図表2：人間の特性カテゴリおよび悪用可能な状況の例

性格	職場	瞬間	状況
役立つ	新入社員	疲労	衝突を嫌がる
騙されやすい	日常業務	大慌て	無謀
好奇心が強い	問題解決スキル	性急	反射的
公平	見知らぬ人とのやり取り（顧客、同僚など）	注意力散漫	驚愕
影響されやすい	不満足	休日	責任回避
内気	余裕	休暇	妥協
油断	恐喝	病欠	協調的
熱心	競争意識	展示会	怒り

と考えるため、その手口に引っかかり、要求されたデータを提供する可能性があります。とりわけ、正しくない要求を確認する習慣がなく、セキュリティ意識が不足している場合には、格好の餌食となってしまいます。

人格特性

人格特性は、最も基本的な人間の特徴です。すべての人が人格特性を持ち、変えるのは一般的にとても難しく、不可能なことさえあります。例として、面倒見の良さ、好奇心の強さ及び公平さがソーシャルエンジニアによって最も悪用されやすい特性です。面倒見の良さは、攻撃者が建物に侵入しようとしたり、電話で他者を装ったりするときに付け込まれます。好奇心の強さは、ターゲットの搾取、マルウェアの拡散もしくはフィッシング攻撃に利用されます。

職場特性

特定の特性や状況は、事業体内の特定の職場や職位に関連します。労働条件に応じて、こうした特性は、従業員が職位、仕事、プロジェクトを変えたときなど、時間の経過と共に変化する可能性があります。新入社員は、すべての同僚と顔見知りではなく、詐欺、電話によるなりすまし要求や電子メール詐欺の被害者になりやすいため、攻撃者にとって垂涎のターゲットです。しかしながら、これは一過性の状態に過ぎません。新入社員が事業体に溶け込むと、攻撃の成功確率が下がるからです。

その他にもソーシャルエンジニアリング攻撃のターゲットになりやすいのは、顧客サービス担当者などの決まった業務に従事している従業員です。なぜなら、なりすまし要求を排除することが難しいからです。例えば、日常業務でマクロが組み込まれた Excel ファイルを使用する従業員は、悪意のあるマクロコードが組み込まれた疑いがある、またはそう装っている添付ファイルを検出できない可能性があります。また、見知らぬ人（例えば、関連企業や顧客の従業員）と連絡を取ることが多い従業員や、電話や電子メールでしか他の施設の同僚と連絡したことがない従業員も、とりわけ面倒見が良かったり、注意力散漫だったりする場合には騙されやすいでしょう。こうしたターゲットには、普通ではない要求、電話/電子メール詐欺、個人攻撃が成功しやすい可能性があります。

労働条件や給与に不満があるなどの否定的な態度も、このカテゴリに関連付けられ、極端な場合には賄賂や恐喝などの犯罪に悪用される可能性があります。特定の職位に就いている従業員について、特定の適性が必須または有利である場合、職場特性と人格特性を調整することが重要になります。

短期特性

通常、この特性は短期で、条件に応じてすぐに変化します。例えば、従業員は残業が多いせいで疲労が溜まり、注意力散漫になることがあります。休暇を取ったり病欠したりすると、攻撃者は不在の従業員とその代理を両方とも悪用できます。攻撃者は休暇中の従業員に電話をかけ、すぐに問題解決を迫ったり、直ちに要求を満たすように強いたりします。その際、その従業員は問題解決を焦る余り、攻撃者を代理者に委ねたり案内したりする可能性があります。また、攻撃者が欠勤している従業員の自動応答により有益な内部情報（代理者の連絡先情報、プロジェクト、タスクなど）を集めようとする場合もあります。この状況は、代理者が要求の信憑性を確認しなかったり、欠勤している同僚や適切な上司を騒がせたりしたくない場合に悪用されます。

このような短期特性に共通するのは、断続的で、せいぜい数日または数週間しか継続することはなく、状況の変化に応じて消え去る点です。攻撃者が短期特性またはそれに関連する状況を特定できる場合、あるいは従業員がいずれかの特性を示していることに攻撃者が気付く場合、攻撃者はターゲットを食い物にする攻撃シナリオを作成できます。

状況特性

状況特性は、セキュリティ侵害などのストレスの多い状況で一般的に発生する短期特性です。状況特性は、攻撃者が敵対的行為を働く手助けをしませんが、攻撃の実施が検出された後に影響を与えるのが一般的であるため、分けて考えられます。一例を挙げると、従業員が疑わしい行為（付添人や入館証なしで外部の者が建物に侵入しようとしている）に気付きながら、問題がない場合の軋轢を避けるために、来訪者（侵入者）に誰何しなかったり、警備員に不審者の報告をしなかったりする場合があります。電話による詐欺の場合、ターゲットの反射的対応が攻撃者にとって有利に働きます。例えば、ソーシャルエンジニアがヘルプデスクの従業員を装い、「あなたのパスワードが漏洩したので直ちに変更してください」と言ってターゲットを脅す場合。狼狽した被害者は、さして考えもせずにパスワードを開示してしまいます（これは、フィッシング攻撃の後で特に有効です）。責任を回避することがマルウェアの感染につながる可能性があります。感染したユーザーは、マルウェア対策ソフトウェアがインストールされているので、悪意のあるコードを特定すべきだったと説明しようとするからです。

従業員のセキュリティ意識向上

従業員は、サイバー攻撃のターゲットになるかもしれませんが、同時に最初の防衛線でもあります。これは、「ヒューマンファイアウォール」と呼ばれることがあります。適切な訓練を受けたセキュリティ意識のある従業員なら、セキュリティイベントやインシデントを予防、検出、報告できます。ファイアウォール、マルウェア対策ソフトウェア、厳格なアクセス権限などの技術的対策は、ソーシャルエンジニアリング攻撃に対して十分ではありません。[13] 従業員は、このような対策を無視したり回避することさえあり、誤ったセキュリティ感覚が育まれています。例えば、ユーザーは、マルウェア対策ソフトウェアがどんな悪意のあるコードやアクションも検出するはずと信じて、疑わしい電子メールのリンクや添付ファイルを開く場合があります。唯一の効果的なソリューションは、ユーザーのセキュリティ意識を高め、セキュリティに対して敏感にさせることです。各事業体では、詐欺、不正、フィッシング、物理的侵入などの人間による攻撃を防ぐために、おかれた環境に合わせてカスタマイズされた独自のセキュリティ意識向上プログラムを策定しなければなりません。

「最上の情報セキュリティトレーニングは、それぞれの役割、責任、役職固有の人的特性および習慣、職場状況、モチベーションを考慮し、対象者に合わせてカスタマイズされます」

セキュリティ意識向上トレーニングには、ポスターやニュースレター、グッズなどの標準的なトレーニングコンテンツ以上のものを含めるべきです。テストや監査の結果を提示するなど、実際の問題を強調し、ゲーム化されたプログラム要素を盛り込むべきです。[14] セキュリティ意識向上トレーニングの主な目的は、情報セキュリティポリシーおよび適用される規制に基づいた責任意識を従業員に伝えることです。これには、セキュリティ規則が必要な理由、現在使用されるサイバー攻撃やソーシャルエンジニアリング技法の種類、従業員が協力して人的リスクを低減する方法についての説明が含まれます。

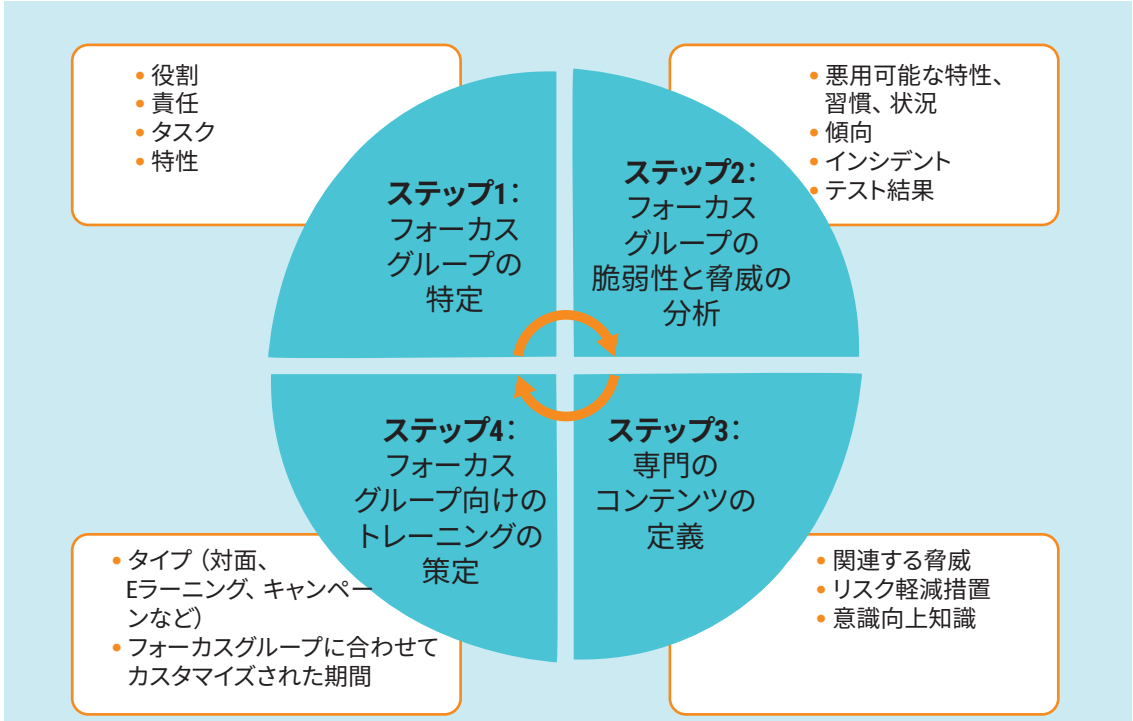
最上の情報セキュリティトレーニングは、それぞれの役割、責任、役職固有の人的特性および習慣、職場状況、モチベーションを考慮し、対象者に合わせてカスタマイズされます。したがって、トレーニング資料および教育フレームワークは、特定のユーザーグループに合わせてカスタマイズすべきです。**図表 3** は、特殊なセキュリティ意識向上トレーニングプログラムを策定する方法を示しています。ステップ 1 では、事業体は、職場での役割と責任、特別な特性や性格に基づいてフォーカスグループを特定します。フォーカスグループの定義に関する推奨事項を以下に記します。

- 管理職
- 見知らぬ人とコミュニケーションを取ることが多いユーザー（管理職補佐、マーケティング/広報部門、顧客サービス、受付など）
- 決まった業務を行うユーザー（管理者、営業担当者、ヘルプデスクなど）
- 特権を持つユーザー（システムオペレーター、IT管理者など）

Enjoying this article?

- Read *A Holistic Approach to Mitigating Harm From Insider Threats. www.isaca.org/insider-threats*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

図表3：セキュリティ意識向上トレーニング



- 可能であれば細分化された特殊トレーニング資料を用いるバックオフィスワーカーや他の分野・部門の従業員（弁護士、財務エキスパート、開発者、アナリストなど）
- 新入社員

ステップ 2 では、事業体は、各フォーカスグループの弱点（脅威、脆弱性、悪用可能な人間の特性、習慣、状況）を分析します。加えて、傾向、過去のセキュリティインシデントやイベント、セキュリティ意識測定結果に基づき、リスクを低減するための対策を考慮するべきです。セキュリティ意識レベルを定期的に測定することは、トレーニングの効果を判定するためだけではなく、弱点やリスク要因、実際の問題を浮き彫りにする専門の教育資料を作成するためにも重要です。事業体内または世界中の過去のセキュリティインシデント、アンケートによる意識向上テスト、観察、ソーシャルエンジニアリング監査結果からデータを集めることができます。

ステップ 2 の結果に基づき、ステップ 3 では各フォーカスグループにとって最も重要な知識を定義します。参加者は、専門の資料を用いることで、実際の脅威や攻撃をよりよく理解し、より効果的に保護対策や検出方法を使用できます。コンテンツの内容と深さは、参加者の役割、責任、職場特性、典型的な脅威に応じて、フォーカスグループごとに異なります。人間による攻撃、脅威、保護/防衛対策を提示するほかにも、トレーニング資料には、情報セキュリティにおけるユーザーの役割やセキュリティ意識向上の利点を取り入れるべきです。ステップ 4 では、ターゲットグループに応じたトレーニング方法とトレーニング期間を決定します。トレーニング方法は以下のとおりです。

- 対面教育またはプレゼンテーション
- 自己学習用Eラーニング
- 対話型ワークショップ
- 意識向上キャンペーン要素

ユーザーが意識向上トレーニングを受けたことがない場合、対面トレーニングが最も有効です。トレーニングが新入社員向けコースの場合、E ラーニングや実際の脅威だけに焦点を絞った短めのプレゼンテーションの方が適切でしょう。例外的なトレーニング（例えば、実際の攻撃後など）の場合、ニュースレターやブログ記事などのキャンペーン要素を使ってもよいでしょう。対象者の需要と要件を識別・評価し、対象者に応じた方法を使用することも推奨します。

一般的に、初回トレーニングプログラムの所要時間は、モジュール式の構造でない場合、グループまたは内容に応じて 1〜2.5 時間ほどです。モジュール式の構造の場合、各トレーニングセッションの所要時間は 30〜45 分までとし、毎月または四半期ごとのペースで開催すべきです。通常、管理職のトレーニングの所要時間は 30〜45 分ほどで、マネージャに影響を及ぼす脅威、各役割の特別な支援的・模範的性質を重点的に学びます。

サイバーセキュリティ月間やサイバーセキュリティ週間などのセキュリティ意識向上キャンペーンでトレーニングセッションを補うことができます。このようなキャンペーンにより、ユーザーは自らのセキュリティ意識を保ち、トレーニングで学んだことやセキュリティが重要である理由を思い出しやすくなり、実践的な体験を得る機会にもなります。セキュリティ意識向上キャンペーンおよびプログラムには、人的要因を悪用する攻撃に対する注意を喚起するトレーニングセッション、特別なプレゼンテーション、ポスター、情報セキュリティ規則に関するスクリーンセーバー、ニュースレター、ブログ、グッズ、クイズ、オンライン/オフラインゲームが含まれます。モバイルアプリケーションやセキュリティ意識向上の逸脱機会などの対話型プログラムが好まれるようです。[15] ユーザーからのフィードバックによれば、これまでによく使用されてきた要素（ポスター、ニュースレター、スクリーンセーバーなど）は、不要な情報や常識的な手順ばかりを提供するため、セキュリティ意識を向上させる方法としてはあまり効果的ではありません。

効果的なセキュリティ意識向上プログラムは、参加者に自身の脆弱性および悪用可能な特性や習慣を認識させます。これにより、悪意のあるソーシャルエンジニアリング攻撃に対して自身を保護することに役立ちます。

結論

従業員は情報セキュリティの重要な要素です。攻撃の潜在的なターゲットとなるだけではなく、ヒューマンファイアウォールでもあります。被害者にならないようにするため、ユーザーは自らの弱点、悪用可能な特性や悪癖を知り、どのような種類の攻撃が自らの脆弱性を悪用するかを認識すべきです。職場環境では、一部のユーザーグループに特定のよく知られた悪用可能な特性や特徴があるため、その従業員に合わせて自らの脆弱性に焦点を絞ったセキュリティ意識向上プログラムをカスタマイズすることが重要です。適切な構造のターゲットを絞ったセキュリティ意識向上トレーニングプログラム、ワークショップ、キャンペーンを完了したら、参加者は規則をより一層遵守するようになり、セキュリティを十分に意識した行動をより一層実践するようになります。

後注

1 Mitnick, K. D.; W. L. Simon; *The Art of Deception: Controlling the Human Element of Security,* Wiley, USA, 2003
2 Verizon, *2020 Data Breach Investigations Report,* USA, 2020, *https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf*
3 PurpleSec, “2021 Cyber Security Statistics: The Ultimate List of Stats, Data and Trends,” USA, 2021, *https://purplesec.us/resources/cyber-security-statistics*
4 Nobles, C.; “Botching Human Factors in Cybersecurity in Business Organizations,” *Holistica,* vol. 9, iss. 3, 2018, p. 71–88
5 Fandi, A.; “Cybersecurity Is More Than Bits and Bytes, It’s Also People and Process,” LinkedIn, 30 September 2019, *https://www.linkedin.com/pulse/cybersecurity-more-than-bits-bytes-its-also-people-process-fandi*
6 Oroszi, E. D.; “Social Engineering Techniques: Targeted Cyberattacks,” National University of Public Services, Budapest, Hungary, 2018
7 Soto, C. J.; “Big Five Personality Traits,” *The Sage Encyclopedia of Lifespan Human Development,* Sage, USA, 2018
8 *Ibid.*
9 Inscape Partners, “The DiSC Model,” *https://ipbpartners.eu/public/artikkel/DiSC_theory__background.pdf*
10 Erős, I.; M. Jobbágy; “A Myers-Briggs Típus Indikátor (MBTI) Magyarországon,” *http://www.mentalhub.hu/mbti.pdf*
11 Mann, I.; *Hacking the Human,* Gower, UK, 2008
12 *Op cit* Oroszi
13 *Op cit* Mitnick
14 *Op cit* Oroszi
15 Oroszi, E. D.; “Make Security Awareness an Experience,” ISACA Now, 25 September 2020, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/make-security-awareness-an-experience*