– CARL SHAPIROとHAL VARIANここ数年、私が確信していることは2つあります。高保証ソフトウェアに対する社会的ニーズが高まっていること、そして市場の力がそれを提供することは決してないということです。  
–伝統的な17世紀8。  
実際、セキュリティメカニズムは多くの場合、責任をシフトするために意図的に設計されており、さらに深刻な問題につながる可能性があります。  
 しかし、複数の所有者がいる複雑なシステムで生じる悪質なインセンティブは、エコノミックな質問をセキュリティエンジニアにとってより重要かつより微妙なものにします。  
2。  
 私たちが得る結果は、通常、市場の均衡であり、多くの場合、驚くほど安定しています。  
マクロレベルでは、テクノロジーが完全に変化し、電話がラップトップに置き換わり、社会がソーシャルネットワークに移行し、サーバーがクラウドに移行したにもかかわらず、サイバー犯罪のパターンは2010年代を通じて著しく安定しています。  
一般的に、インセンティブがない限り、人々は行動を変えません。  
 しかし、市場は失敗する可能性があります。コンピュータ業界は、創業当初から独占企業に悩まされてきました。  
セキュリティ経済学は、2000年代初頭以来、学問分野として急速に発展してきました。  
 たとえば、プログラマーとテスターに​​よる最適なバランスはどのくらいですか？ （答えについては、セクション8を参照してください。  
以下の3。  
 そして、保護メカニズムを使用して、所有物またはデータで誰かが実行できることを制限する場合、競争政策と消費者の権利に関する質問が続きます。これを分析するには経済学が必要です。  
この章では、まず、古典経済モデルで独占を分析する方法、情報商品とサービス市場がどのように異なるか、ネットワークの影響と技術的なロックインによって独占が起こりやすくなる方法について説明します。  
 次は、人々が協力するか競争するかを分析できるゲーム理論と、インターネットの大部分を牽引する広告市場の仕組みを理解することを可能にするオークション理論と、それらがどのように失敗するかです。  
 また、システムが本来よりも信頼性が低い理由、つまり脆弱性が多すぎる理由、およびサイバークロークが捕捉されない理由を理解することもできます。  
2古典経済学現代経済学は、人間行動の多くの異なる側面をカバーする巨大な分野です。  
 このセクションでは、ミクロ経済学からの最も関連性の高いアイデアのヘリコプターツアーから始めます。  
2。  
現代の主題は、貿易の成長が世界を変え、産業革命につながり、人々が起こっていることを理解したかった18世紀に始まりました。  
 専門化は生産性の向上につながります。人々は競争の激しい市場で生き残るために他の価値のあるものを生み出そうとします。  
同じメカニズムがファーマーズマーケットや小規模な工場から国際貿易まで拡大します。  
 JevonsとMengerからの洞察の1つは、競争の激しい市場で平衡状態にある良品の価格は、生産の限界コストであるということです。  
 価格が下がった場合、これらの鉱山は閉鎖されます。それが上がった場合、さらに多くの限界鉱山が開かれます。  
 （また、今日の多くのオンラインサービスが無料である理由についての洞察も得られます。情報を複製するための限界コストはほぼゼロであるため、多くのオンラインビジネスは情報を販売できず、広告などの他の方法でお金を稼ぐ必要があります。  
）世紀の終わりまでに、アルフレッド・マーシャルは、商品、労働力および資本の市場における需給のモデルを、均衡においてすべての過剰な利益が競い合わされ、経済が競争する包括的な「古典的」モデルに結合しました効率的に機能します。  
経済学への関心の多くは、これらの条件の1つ以上が満たされていない状況に由来しています。  
エコノミストはこれらの外部性を呼びます、そしてそれらはポジティブまたはネガティブのいずれかです。  
 結果として、研究者は彼らの研究の利益を完全に捉えることができず、理想よりも少ない研究しか得られません（経済学者は、理想的な量の研究の4分の1しか行わないと考えています）。  
セキュリティエンジニアリング265ロスアンダーソン8。  
 古典的な経済外部性およびその他の市場の失敗の原因は、コンピュータ業界、特にセキュリティ関係者にとって非常に重要です。これらは、業界の独占から安全でないソフトウェアに至るまで、私たちが取り組む多くの問題を形作るためです。戦略とは、権力を獲得すること、または他の人々があなたに対して権力を持つことを防ぐことです。したがって、最も基本的なビジネス戦略は、余計な利益を引き出すために市場力を獲得すると同時に、他者へのあなたの活動のコストを最大限に分配することです。  
8。  
1独占導入として、独占の教科書ケースを考えてみましょう。  
 1人の金持ちの学生が1か月に4000ドルを支払うことができ、300人が少なくとも月に2000ドルを支払うことを望んでいて、少なくとも1000人が少なくとも月に1000ドルを支払う準備ができているかもしれません。  
1以下。  
1：アパートの市場したがって、競合する家主の多くが1000のアパートを賃貸している場合、市場清算価格は、需要曲線と垂直供給曲線の交差点、つまり$ 1000になります。  
 独占的な家主が需要曲線を調べたところ、賃貸しているアパートが800室しかない場合は、それぞれのアパートで月額1400ドルを稼ぐことができます。  
 （経済学者セキュリティ工学266ロス・アンダーソン8。  
 クラシック経済学では、彼の「収益ボックス」は、図8のEDGOではなくボックスCBFOであると言うでしょう。  
）それで、彼は人工的に高い値段を設定しました、そして、200のアパートは空のままです。  
 パレート改善は、一部の人々を他の人を悪化させることなくより良いものにするあらゆる変更であり、利用可能なパレート改善がない場合、同種カチオンはパレート効率的です。  
 NowPareto効率は、かなり弱い基準です。完全な共産主義（誰もが同じ収入を得る）と完全な独裁政権（国王が多くを得る）の両方がパレート効率的です。  
では、独占者は何ができるのでしょうか？ 1つの可能性があります。彼がすべての人に異なる価格を請求できる場合、彼は各学生の家賃を彼らが支払う準備ができているものに正確に設定できます。  
 同じ学生は以前と同じようにアパートを取得しますが、ほとんどすべての学生はより悪いです。  
 差別的な独占者はなんとかしてすべての消費者余剰を抽出する。  
 あなたが彼の価格を値下げすることを期待しているカーペット売り手イスタンブールは、最初に、ビジネスと牛のクラスの座席を販売する航空会社と同様に、このゲームをプレイしています。  
 市場支配力は、商人が独占者であることへの近さの尺度です。独占の下では、商人は価格設定者ですが、完全な競争の下では、市場が確立するどんな価格でも受け入れなければならない価格担当者です。  
 情報の非対称性は、いくつかの方法でそれらを助けることができます。  
 そのため、商人は固定価格を表示するよりも、せりふを好むかもしれません。  
 価格比較サイトのおかげで、その乗客は基本価格についての良い情報を持っていますが、満席に割引をする場合、広告エコシステムからの情報を使用してその顧客をターゲットにできるかもしれません。  
 テクノロジーは、企業を航空会社に似たものにし、小さなカーペット店に似たものにしないように傾向があります。情報の非対称性は、平均価格について知っているかどうかに関係なく、システムがユーザーについて知っていることと、システムがユーザーを固定する方法と同じです。  
 家主やこの例のカルテリンのような古典的な独占者は、単にすべての人の価格を押し上げるため、消費者余剰が明らかに失われる可能性があります。  
19世紀後半、鉄道事業者は、収益性や商品の腐りやすさなどの要因に応じて、さまざまな顧客にさまざまな運賃を請求しました。基本的には、セキュリティエンジニアリング267ロスアンダーソン8に従ってすべてを揺さぶっています。  
 情報経済学の支払い能力。  
同じように、電話会社は狂ったように価格差別をしていた。 SMSは以前は音声よりもはるかにコストがかかり、音声はデータよりもはるかに多く、特に距離が長い場合はそうでした。  
 これはまだ乱闘スペースであり、FCCのトランプ大統領の任命者は以前の多くの正味の中立性の決定を覆しました。  
 これは、アメリカでは少なくとも経済学者や弁護士が独占について考えていた伝統的な根拠に挑戦しています。  
 1970年代に1人の支配的なプレーヤー（IBM）から1990年代に2人（MicrosoftとIntel）になり、現在は少数（Google、Facebook、Amazon、Microsoft、maybeNet ﬂ ix）になっているかもしれませんが、それぞれがその分野を支配しています。 ArmはIntelとの競争に成功しましたが、2009年のBing以降（市場シェアが下がっています）、2011年のInstagram（現在はFacebookが所有）から大きなソーシャルネットワークはありません。EUは、技術者たちに何度も競争条件を定めてきました。  
8。  
 コンピュータが登場する以前から、新聞は大都市を除いて独占的である傾向がありました。  
 19世紀後半に電気式の集計機器が登場したとき、IBMと呼ばれるNCRのマンハッタンの販売店からのスピンオフが引き継がれるまで、NCRが支配していました。  
 それ以来、GoogleとFacebookが広告を支配するようになり、AppleとGoogleが電話オペレーティングシステムを販売し、ARMとIntelがCPUを提供する一方で、他の多くの企業が独自の専門分野を支配しています。  
3。  
 しかし、ほとんどゼロの情報については！そのため、オンラインには無料のものがたくさんあります。ゼロはその公正価格です。  
例として百科事典を考えてみましょう。 Britannicaは、32巻で1,600ドルの費用がかかりました。その後、MicrosoftはEncartaを49ドルで売り出した。  
3。  
 企業は次々に、商品が無料で配られ、そのお金は広告や並行市場で得られるビジネスモデルに移行する必要がありました。  
 そのため、固定費が高く限界費用が低い他の業界、たとえば新聞、航空会社、ホテルなどが集中する傾向があります。  
 電話や電子メールなどのネットワークは、最初は話をする愛好家が数人しかいなかったため、利用に時間がかかりましたが、各ソーシャルグループで一定の基準を超えると、全員が参加する必要があり、ネットワークは急速に主流になりました。  
 この肯定的なフィードバックは、ネットワーク効果が確立されるメカニズムの1つです。  
 たとえば、地元の新聞が19世紀に入ったとき、企業は多くの読者がいる新聞に広告を掲載したいと考えていました。  
 鉄道が農業の工業化を可能にしたとき、同じことが起こりました。 Cargilland Armorのような強力な企業は、穀物エレベーターとミートパッカーを所有しており、一方では小規模農家を、もう一方では小売業界を扱っていました。  
 PCが登場したとき、Microsoftは同じ理由でAppleを打ち負かしました。携帯電話がラップトップに取って代わった今、AndroidとiPhoneでも同様のパターンが見られます。  
 ネットワーク効果もマイナスになる可能性があります。 MyspaceなどのWebサイトがカスタムを失い始めると、negativefeedbackはその損失を大敗に変える可能性があります。  
 これらにより、サービス提供者の競争上の優位性を早期に獲得し、現職者が防御することができます。  
ソフトウェア会社が製品にWindowsやOracleなどのプラットフォームの使用を約束すると、変更に費用がかかる可能性があります。  
 同じことが顧客にも当てはまります。新しいソフトウェアや変換ファイルを購入する必要があるだけでなく、ステータスも再トレーニングする必要がある場合、販売を完了するのが難しい場合があります。  
 相互運用性が重要であった以前のプラットフォームには、電話システムのセキュリティエンジニアリング269ロスアンダーソン8が含まれていました。  
 情報経済テレグラフ、幹線電力、さらには鉄道。  
 ユーザーが他のユーザー（およびソフトウェアなどの補完的な製品のベンダー）との互換性を望んでいる場合、最大の市場シェアを獲得すると期待しているベンダーから論理的に購入します。  
3。  
 これがどのように機能するかを確認するために、Oceを使用する各100ステイのファームを検討してください。  
 しかし、切り替えのコストが15,000ドルを超える場合、Microsoftはその価格を引き上げます。  
 この本の第2版では、この例のOceのコストは500ドルでした。それ以来、Oceと同じように機能するGoogleドキュメントなどのクラウドベースのサービスにより、切り替えのコストが削減されたため、Microsoftは価格を大幅に削減する必要がありました。  
99と164ポンド。  
 オンラインサービスに年間30ドルを請求することは、顧客が5年間または7年間使用する可能性のあるプログラムに60ドルを請求するよりも優れています。  
 新しい形式のロックイン、つまり、クラウドプロバイダーがすべてのデータを管理するようになりました。  
 また、クラウドへの移行を説明するのにも役立ちます（ただし、コスト削減はより大きな推進力です）。  
 そのような場合、可能性のある攻撃者は悪意のある外部者ではなく、機器の所有者、または互換性のある製品を作成することによって既存企業に挑戦しようとする新しい企業です。  
 イノベーションはしばしば段階的であり、新しい企業がそれらのためのキラーアプリケーションを見つけたときに製品が成功するので、物事を厳しく制限することもビジネスに悪影響を及ぼす可能性があります[903]。確かに、IBM PCがApple Macよりもオープンであるという事実は、その支配的なデスクトッププラットフォームになる要因の1つでした。  
3。  
）そのため、多くの国の法律により、企業は互換性のために競合他社の製品をリバースエンジニアリングする権利を与えられています[1647]。  
 クラウドサービスや暗号化などのデジタルコンポーネントを使用して製品をロックダウンしているため、競合他社がこれらの製品のリバースエンジニアリングを試みる法的権利を有していても、実際に成功するとは限りません。  
 これらのより複雑なエコシステム戦略については、セクション8で詳しく説明します。  
4。  
3。  
 私たちは、昔ながらのカーペットトレーダーが、自分の店で買い物をする観光客よりも情報の利点を持っていることを話し合いました。しかし、非対称情報の正式な研究は、1970年に「レモンの市場」に関する有名な論文[34]によって蹴られ、ジョージアケルロフがノーベル賞を受賞しました。  
 売り手はどちらがどちらかを知っていますが、買い手は知りません。  
 したがって、市場価格は$ 1000近くになります。  
 非対称情報は、貧弱なセキュリティ製品が一部の市場を支配している理由でもあります。  
 1990年代にアンチウイルスソフトウェアの市場が衰退したとき、人々は20ドルではなく10ドルの製品を購入しました。  
人々が依然として大量のAVを購入していることは、非対称情報のもう1つの例です。  
 たとえば、ボルボは、乗員が事故に耐えるのに役立つ安全な自動車を製造することで定評がありますが、ボルボの運転手は事故を増やしています。  
 どちらの効果もセキュリティ上重要であり、特定のケースでは両方が組み合わさることがあります。  
 これは、強制的なシートベルト法が全体の命を救うのではなく、単に車両乗員から歩行者や自転車に死者を移動させる傾向がある理由も説明しています[19]。  
3。  
 情報セキュリティの世界では、ほとんどの利害関係者が真実を伝える意欲がないために、事態はさらに悪化しています。警察、諜報機関、およびセキュリティベンダーは、ソフトウェアベンダー、eコマースサイト、および銀行が脅威を軽視している間、脅威について語ろうとします[111]。  
3。  
 典型的な例は、大気質、国防、科学的研究です。  
調整されていない市場は一般に社会的に最適な量で公共財を提供することができません。  
 非常に頻繁に、公共財は公的および私的な行動のいくつかの組み合わせによって提供されます。科学的研究は、いくらかの公的助成金を得て、学生料金からいくらかの収入を得て、そして産業からいくつかの研究契約を得る（有用な発明の特許を得るかもしれない）大学で行われます。  
 私の家の屋根には対空砲はありません。航空防衛の脅威は少数の攻撃者からのものであり、政府の行動によって最も効率的に対処されます。  
 自己防衛には公共財のいくつかの側面がありますが、保険は私財です。  
 セクション2のサイバー犯罪の簡単な調査で。  
 2007年までに深刻なスパマーシャッドの数は一握りになり、2019年にはサービス拒否（DoS）攻撃でも同じことが起こりました。1つの主要なDoS for-hireプロバイダーが存在するようです。  
脆弱性を発見した研究者に報酬が支払われ、ソフトウェアがそれらを含んでいる企業に課された罰金によって支払われる、より穏やかな政府の対応を想像した人もいます。  
しかし、皮肉屋は実際に起こることは脆弱性がサイバー武器メーカーに売られ、政府がそれらを備蓄してそれらを備蓄していることを指摘します-そして業界はNotPetyaのように付随的損害の支払いをします。  
4。  
8。  
それは、私たちが協力するときと、戦うときです。  
 あなたは何か有用なものを作り、それを交換します。または、必要に応じて、強制的に、投票箱などを使用します。  
それらを調査および分析するために使用できる主なツールは、ゲーム理論です。独立した意思決定者間の協力と衝突の問題の研究です。  
 私たちは戦略ゲームに興味があり、細部の大部分を抽象化して決定の核心に到達しようとします。  
これを図7のように記述します。  
2 –一致するペニー表の各エントリは、最初のアリスの結果、次にボブの結果を示しています。  
 これはゼロサムゲームの例です。アリスの利益はボブの損失です。  
ここに例があります（図7。  
3-支配的な戦略の均衡ゲーム理論では、戦略はゲームの状態とセキュリティエンジニアリング273Ross Anderson8をとるアルゴリズムにすぎません。ゲーム理論は移動を出力します1。  
 各プレイヤーには支配的な戦略があります。他のプレイヤーが何をするかに関係なく、最適な選択です。  
 これを支配的な戦略均衡と呼びます。  
4：BobAliceLeftRightTop2,10,0Bottom0,01,2図7。  
 アリスの選択がボブの場合に最適である場合、およびその逆の場合、2つの戦略はナッシュ均衡にあると言います。  
 支配的な戦略の均衡がグローバルな最適である一方で、それらをローカルのオプティマのように考えることができます。  
4。  
 それは、1950年に米国とソ連の防衛支出の文脈で最初にtheRand社の科学者によって研究されました; Randは核戦争における可能な戦略について考えるために支払われました。  
銀行強盗を計画している疑いで2人の囚人が逮捕されました。  
 1人だけが告白した場合、彼は自由になり、もう1人は陰謀犯のために6年の猶予があります。  
」囚人たちは何をすべきか？これが彼らの支払い行列です：BenjyAlfieConfessDenyConfess-3、-30、-6Deny-6,0-1、-1図7。  
セキュリティエンジニアリング274ロスアンダーソン8。  
 ゲームの理論1年をやるのではなく歩くので、私はまだ告白すべきです」  
 2人は告白し、それぞれ3年の猶予があります。  
 各囚人は、他の囚人が何をするかにかかわらず、告白するべきです。  
 （これは、「最高」について論じるだけでなく、「パレート効率」や「支配的戦略均衡」などの概念を持つことが有用である理由の1つです。  
 どちらの囚人も自白し、3年の刑期を迎える。  
 ただし、囚人のジレンマは、協力するかどうかを決定するあらゆる種類の相互作用をモデル化するために使用できます。国際貿易、核兵器管理、漁業保護、CO2排出量の削減、政治談話の礼儀正しさなどです。  
 これらのアプリケーションでは、私たちは良い結果を得ることができるように協力を望んでいましたが、シングルショットゲームの構造によっては、それらを実現するのが非常に難しくなる場合があります。  
多くの可能性があります。貿易に関する国際条約から暴力団の通商法まで、さまざまな種類の法律が存在する可能性があります。  
8。  
2反復ゲームと進化ゲームゲームを繰り返しプレイするとします。アルフィーとベンジーはお互いに何度もやり取りすることを期待しているキャリア犯罪者だとしましょう。  
これをモデル化するには、少なくとも2つの方法があります。  
 彼は人々がプログラムを提出することができる一連の競争を設定し、これらのプログラムはトーナメントでお互いに繰り返し遊んだ。  
 戦略の進化が多くのことを説明できることに気づき始めました。  
 したがって、この場合、他のプレーヤーを時々「許す」ことが役立ちます。  
 彼らは、攻撃的で従順な個人、「タカ」と「ハト」の混合集団があり、それらが協力する行動をとるとどうなるかを考えました。鷹は鳩から餌をとります。セキュリティエンジニアリング275ロスアンダーソンのリスクがある鷹との戦い8。  
 ゲーム理論死。  
 すると、payo↵マトリックスは図7のようになります。  
6 –鷹狩りゲームここで、v> cの場合、ドミナント戦略であるため、全個体数が鷹になりますが、c> v（戦いが高すぎる）の場合、鳥の確率pは鷹であり、鷹のpayo payとdovepayo↵を等しく設定します。つまり、ispv�c2 +（1�p）v =（1�p）v2であり、p = v / cによって解かれます。  
 もちろん、コストは時間の経過とともに変化する可能性があり、戦争が勃発したときに一部のハードマンとの不安が有利になる可能性があるため、多様性は進化論的には良いことです。  
 恐らく、侵略の現在の高い発生率は、前国家社会の状態を反映しています。  
 私たちは、進化が追いつくために文明社会に長く住んでいませんでした。  
彼らは、協力がどのように発展したかについてのさらなる洞察を提供します。  
公平性は、さまざまなレベルでさまざまな方法で機能します。  
 eBayによって開拓され、UberやAirBnBなどの企業によって現在使用されているオンラインレピュテーションシステムは、同様の機能を実行します。つまり、反復ゲームへの対話を行うことで、タカを回避します。  
 旧約聖書には「目のための目」があり、新約聖書には「あなたがたにしてもらいたいように他人にやる」-後者の方がフォールトトレラントである-とそのバージョンは孔子のアリストテレスにありますと他の場所。  
5。  
9月11日以降、人々は鷹の巣のゲームを使用して、ストレスの時に信仰の言説を引き継ぐ原理主義者の能力をモデル化してきました。進化的ゲームは、秘密の取引がない業界でもカルテルのような行動が見られる理由を説明しています。  
 ローカルループでISPに月6ポンドの費用がかかる場合、ISPsallの料金は35ポンドになるのはなぜですか？  
そして、航空会社が顧客を混乱させるためにあらゆる種類の取引や航空マイルなどを提供するのと同様に、通信事業者も独自の混乱価格を提供しています。  
 暗黙の共謀は、企業の幹部が実際に座って価格を修正することに同意することなく両方の業界で発生する可能性があります（これは違法になります）。  
8。  
 多くのオンライン活動は、GoogleやFacebookのような企業が運営する広告オークションによって賄われており、多くのeコマースサイトはオークションとして運営されています。  
 これらは、ユニークな商品の価格を見つけるための基本的な方法です。  
以下の5つの従来のタイプのオークションを検討してください。  
 英語または昇順オークションでは、競売人は最低価格で開始し、入札者が1人だけになるまで価格を上げます。  
2。  
 これは販売業者に使用されます。  
 最初の価格の密閉入札オークションでは、各入札者は1つの入札を行うことができます。  
セキュリティエンジニアリング277ロスアンダーソン8。  
 オークション理論これ​​はテレビの権利のオークションに使用されています。政府契約にも使用され、落札した最低入札価格です。  
 セカンドプライスの密閉入札オークション、またはビックリーオークションでは、入札をゲットして最高入札額が落札されますが、その入札者は2番目に高い入札額で価格を支払います。  
5。  
 これは、いくつかのハイテクスタートアップ間の戦争、訴訟、または勝者独占市場競争のモデルです。  
最初の重要な概念は、戦略的同等性です。  
 同様に、イングリッシュオークションとヴィックリーオークションの結果は同じです（入札単価の増分を法として）。  
 オランダのオークションでは、評価が他の誰よりもはるかに高いと思われる場合は安く入札する必要がありますが、セカンドプライスオークションでは、誠実に入札するのが最善です。  
 これは弱い概念です。誰が勝つかということではありませんが、オークションでどれだけの金額が集まると期待されていますか。  
これらの条件には、リスク中立入札者、共謀なし、パレート効率（最高入札者が商品を手に入れる）、および独立評価（入札者間の外部性なし）が含まれます。  
 したがって、オークションを設計するときは、条件が理想的でない方法に焦点を当てる必要があります。  
そして、うまくいかないことがたくさんあります。  
 第2に、売買の検出があります。英国のテレビの権利に関する1つのオークションでは、入札者は制作会社との話し合いを含む広範なプログラミングスケジュールを提出する必要があり、業界の誰もが誰が入札しているかを知っていて、入札者が1人だけのフランチャイズはピーナッツに行きました。  
 第4に、リスク回避策があります。$ 2の50％の確率よりも$ 1の特定の利益を好む場合は、ファーストプライスオークションでより高い価格で入札します。  
 また、予算にも制約があります。入札者が現金で制限されている場合、全額オークションのほうが収益性が高くなります。  
Security Engineering278Ross Anderson8が開発した広告オークションメカニズム。  
 セキュリティと信頼性の経済性Googleは、収益を最適化するために調整されたセカンドプライスオークションです。  
 次に、「広告ランク」をai = bieiとして計算します。  
 したがって、これはセカンドプライスオークションですが、biではなくaiのランキングに基づいています。  
 これは、妥当な仮定の下で、プラットフォームの収益を最大化することを示しています。  
 メディアがソーシャルになると、広告の品質は簡単にバイラリティに切り替わります。  
 1つの結果は、2016年の米国大統領選挙で、ヒラリークリントンがドナルドトランプが払った額よりも多くの広告を支払ったことでした[1234]。  
 一部の人々は、この「配信の最適化」は選挙法で禁止されるべきだと感じています。確かに、効率性と公平性の間に構造的な緊張があるメカニズムのもう1つの例です。  
 たぶんそのような法域で最もクリーンな解決策は、たばこと同じようにそれらをオンラインで禁止することです。  
 さらに、広告主はより「価値のある」人口統計を求めて競争するため、広告効果は性別や人種などの要因によって歪められる可能性があり、広告見出しや画像の魅力のためにコンテンツ効果によっても影響を受けます。これは意図的または偶発的である可能性があり、雇用や住宅を含む幅広い広告に影響を与える可能性があります[39]。8。  
 しかし、1945年以降、核兵器は国の生存を経済力から切り離すと考えられ、経済学と戦略研究の分野はバラバラになりました[1238]。  
2000年頃、私たちの多くは、一見して不合理であるように見える永続的なセキュリティ障害に気づきましたが、さまざまな主体が直面しているインセンティブをより注意深く見たとき、私たちはそれを理解し始めました。  
Hal Varianは、ベンダーが期待するほどウイルス対策ソフトウェアに多くのお金をかけなかった理由を調査しました[1943]。  
6。  
 当時、この本の初版を書いていましたが、問題の多くをインセンティブ問題として説明することで、説明が説得力を増すことがわかりました。そのため、本の最終的な編集から学んだことを「情報セキュリティが難しい理由-経済的展望」という論文にまとめました。  
 彼らが登場する頃には、9/11攻撃が起こり、人々はセキュリティに関する新しい見方を求めていました。  
（後で、私たちは患者の安全の失敗がしばしば同様の根を持っていることを発見しました。  
 ネットワーキングの研究者たちは、オークション理論を使用して、戦略を証明できるルーティングプロトコルを設計し始めました。  
 マイクロソフトは標準の経済性について考えていました。  
 浮上し始めた絵は、システムのセキュリティが失敗したというものでした。システムを守っている人々は、失敗のコストを犠牲にした人々ではなかったからです。  
 言い換えると、セキュリティはしばしば権力関係です。特定のシステムでそれが何を意味するかを制御するプリンシパルは、しばしばそれを使用して自分の利益を前進させます。  
 しかし、主題を真剣に研究し始めると、それだけではないことがわかりました。  
6。  
マイクロソフトの支配的な市場地位にもかかわらず、Windowsがそれほど安全ではないのはなぜですか？はるかに優れたソフトウェアを作成することは可能であり、防御やヘルスケアなど、信頼できるシステムを生み出すために真剣な取り組みが行われている分野があります。  
 そのようなレースでは、1990年代のマイクロソフトの哲学–「火曜日に出荷してバージョン3までに正しくする」–は完全に合理的な行動です。  
 セキュリティはアプリケーションの邪魔になり、とにかくレモン市場になりがちです。  
6。  
 その後、セキュリティを強化するかもしれませんが、顧客のロックインを最大化するように設計したり、デジタルメディアなどの新しい市場の補完者にアピールしたりする誘惑に駆られます。  
 製品は最初は安全ではなく、時間の経過とともに改善されますが、新しいセキュリティ機能の多くは、ユーザーと同じくらいベンダーの利益になります。  
 DOSにはまったく保護機能がなく、マルウェア市場をけん引しました。 Windows 3とWindows 95は恐ろしいものでした。 Windows 98はわずかに優れていました。そしてセキュリティの問題により、最終的に2003年にビルゲイツはすべてのエンジニアが安全なコーディングコースに入るまで開発を中止することを決定したので、Microsoftの顧客を苛立たせました。  
 悪用可能な脆弱性の数と寿命は、Windowsのその後のリリースを通じて減少し続けました。  
 Peter Gutmannが指摘しているように、ユーザーのクレジットカード番号を保護するよりも、プレミアムビデオコンテンツを保護する方がはるかに効果的です[842]。  
 新しいプリンターを$ 39で購入します。  
各95。  
アプリケーション開発者の観点から見ると、ロックインに基づく標準競争のある市場は、このように見えます。  
 貧困層の消費者の観点からすると、「貧弱なセキュリティ、それから誰かのセキュリティ」と表現することができます。  
 支配的な地位を確立するために競争するとき、ベンダーは製品を設計するように誘惑され、セキュリティ管理のコストのほとんどがユーザーに捨てられます。  
これは1990年代半ばに採用され、MicrosoftとNetscapeがブラウザ市場の優位を争った。  
 それでも、ユーザーのコンプライアンスコストをダンプすることは、当時は完璧でした。 SETのような競合するプロトコルは、オンラインで購入したいすべての顧客に証明書を発行するコストをサドルバンクに課し、コストが高すぎます[524]。  
不良品や商品に対するネットワークの影響もあります。  
セキュリティエンジニアリング281ロスアンダーソン8。  
 感染するWindowsマシンが増えるにつれ、セキュリティと依存性の経済性2010s –ラップトップにもっとお金を払う用意ができていた人々が、ソフトウェアをあまり実行しなかったものであるにもかかわらず、より安全なものを持つことができるという奇妙な均衡につながります。（そこでは、Appleのアプリストアのより厳しいポリシーが市場シェアよりも重要になっています。  
6。  
 脆弱性を発見した場合、それを公開するだけでよいのです。ベンダーにパッチを適用するよう強制する可能性がありますが、そうするまで何ヶ月も人々に公開されたままになる可能性がありますか？または、それをベンダーに非公開で報告する必要があります。そして、誰かに告げれば、弁護士からの手紙で高額な訴訟を脅かす恐れがあります。その後、ベンダーはパッチを適用する必要がありません。この議論は長い道のりです。序文で述べたように、ヴィクトリアンはロックピッキングに関する本を出版することは社会的責任があるのか​​と悩み、結局それは[1895]であると結論付けた。  
セキュリティ経済学は、この種のいくつかの問題を議論するための理論的および定量的フレームワークの両方を提供します。  
 しかし、現実の世界は実際にそのようなものですか？それとも、関連するバグやベンダーの内部知識によって歪んでいるのでしょうか？これは大きな政策論争につながりました。  
 Ashish Aroraや他の人々は、公開によりベンダーがバグをより迅速に修正したことを示すデータで対応しました。攻撃は当初は増加しましたが、報告された脆弱性は時間とともに減少しました[133]。  
 つまり、適切な状況では、ソフトウェアは牛乳よりもワインのようになり、年齢とともに向上します。  
）さらにいくつかの制度的要因が、責任ある開示（調整された開示とも呼ばれる）に賛成して議論を解決するのに役立ちました。それにより、人々はベンダーまたはサードパーティにバグを報告し、パッチが利用可能になるまで機密を保持し、その後、記者にクレジットを提供します。彼らの発見。  
6。  
2。  
3。  
 2つ目は、セキュリティの研究者がバグを販売できる、iDefenseやTippingPointによって設立されたような脆弱性の商用市場の出現です。その後、これらの企業はベンダーに責任を持って各バグを開示し、企業の運用しているファイアウォールまたは侵入検知サービスに販売される可能性のある侵害の兆候を解明します。  
Stuxnetが政府に脆弱性を備蓄させた後、この市場は大幅に拡大しました。  
 これはサプライチェーンにノックオン効果をもたらしました。  
 Sam Ransbothamはすでに2010年に、理想的なモデルではオープンソースソフトウェアとプロプライエタリソフトウェアは同等に安全ですが、オープンソースの世界ではバグがエクスプロイトに早変わりするため、攻撃者はよりターゲットを絞っています[1579]。  
 ベンダーは同等の方法で対応しています：AppleはBlack Hat2019で、iOSでゼロクリックのリモートコマンド実行を可能にするエクスプロイトに対して最大100万ドルになるバグ報奨金スケジュールを発表しました。  
好むと好まざるとにかかわらず、オープンソースプロジェクトを実行しているボランティアは、自分のプロジェクトがどこにでもある場合、有能なやる気のある対戦相手を見つけるようになりました。たとえ彼らがAppleのポケットに収まらなくても、できるだけ多くの研究者を傍らに置いておくことは良い考えです。  
 ベンダーとその顧客の間には、パッチのリリースの頻度とタイミングだけでなく、信頼を補完する補完的なユーザーや二次的なユーザーとの間に緊張があります。  
 Linuxはどこにでも組み込まれています。エアコン、スマートTV、さらには車の中までです。  
 コア開発者が次のパッチリリースについてすべてを信頼するプラットフォームを使用している企業が多すぎる可能性があります。  
 私たちは、携帯電話のブラウザーで使用されているthe3Webkitの複数の重複するエコシステムを研究する必要がありますセキュリティエンジニアリング283ロスアンダーソン8。  
 CVE番号で索引付けされたセキュリティと依存性の脆弱性の経済性;侵入検知システムに供給される侵害の指標（IoC）の;市場、CERT、ISACを介してベンダーに直接開示すること。さまざまなボットネット、犯罪組織、国家の行為者さまざまな記録された犯罪パターンの。  
パートIIIでこのすべてに戻ります。  
6。  
 このように、島の洪水防御は最も弱いつながり、つまり最も怠惰な家族に依存していました。  
 ベストショットのもう1つの例は、2つの軍のチャンピオン間の単一の戦闘があり得る中世の戦争です。  
 中世のヴェネツィアは、洪水の危険のために最も弱いリンク防衛の最も良い例でしたが、中央政府は強力で、商人の家族は洪水の防衛よりも独裁的な権力を持つ総督を選出しました。Hal Varianは、このモデルを情報システムの信頼性にまで拡張しました。パフォーマンスは、最も弱いリンク、最良の出力、または合計の合計に依存する可能性があります[1945]。  
 これはベストショットよりも効率的であり（ほとんどの人はヒーローの背後でフリーライドします）、逆に最も弱いリンクよりも効率的です（誰もが最も怠惰で脆弱になります）。  
 プログラムの正確さは、最も弱いリンク（脆弱性を導入する最も不注意なプログラマー）に依存する可能性がありますが、ソフトウェアの脆弱性テストは、全員の行動の合計に依存する可能性があります。  
 エージェントが追加されると、システムは総和の場合は信頼性が高くなりますが、最も弱いリンクの場合は信頼性がなくなります。  
その他の攻撃と防御のモデルには、マルウェア拡散の流行モデルが含まれます。これは、コンピュータウイルスがフロッピーディスクを介してマシンからマシンに拡散したときに重要でしたが、現在、ワーム化可能なエクスプロイトが比較的少ないため、あまり関心がありません。タイミングに依存するセキュリティゲームのモデル、特にRon Rivestと同僚によるFlipItのゲーム[559]。確かに、ゲーム理論と情報セキュリティに特化した会議全体（Gamesec）があります。  
 たとえば、ほとんどのソーシャルネットワークでは、他のノードへのリンク数が比較的多い比較的少数のノードへの接続が必要です[1994]。  
6。  
 米英軍も同様に、イラク戦争中の反乱鎮圧作戦で高度に接続された人々を標的とした（そして、その結果として生じたスンニ派地域の社会的崩壊はISISの出現を助けた）。  
George Danezisと私はまた、防衛のために連帯が必要な場合、より小さくてより均質なグループがより効果的であることを示しました[511]。  
 例としては、脆弱なパスワードを簡単に推測して、侵害された電子メールアカウントの在庫を補充するスパマーや、eコマースWebサイトに対するカードを提示しない詐欺などがあります[276]。  
これらの機関は、セキュリティの展望を形作ります。  
 ただし、セキュリティエコシステムの最大の機関は、おそらく政府機関ではなく、支配的な企業です。  
6。  
 1980年代には、ファイル形式の戦争が起こり、企業がソフトウェアが生成したワープロファイルやスプレッドシートへのアクセスを阻止しようとしました。  
 ネットワークに影響を与える一種の柔道として浮上した敵対的な相互運用性[570]。  
 初期のセキュリティ経済学論文で、Hal Varianは2002年に彼らの束縛されない使用が競争に損害を与える可能性があると指摘しました[1944]。  
 競争的虐待の明らかな可能性がありました。 Security Engineering285Ross Anderson8のマシンの所有者からユーザーデータの制御を移す。  
 それが格納されているファイルの作成者に格納されるセキュリティと依存性の経済性により、ロックインの可能性が大幅に増加します[73]。  
3。  
彼らがマイクロソフトに支払う15,000ドルは、トレーニングやファイルの変換などを含む、LibreOceへの切り替え（たとえば）にかかる総コストとほぼ同じです。  
現在、IRMはその時点で失敗していました。企業アメリカはそれがロックインプレーであることをすぐに理解し、ヨーロッパ政府はTrusted Computingイニシアチブが小規模企業を除外したという事実に反対し、Microsoftはメカニズムを機能させることができませんでした適切にVista。  
別の側面は、DRMと音楽に関するものです。  
 無許可のピアツーピアのファイル共有がクリエイティブ産業を破壊するというハリウッドの主張は、常に不安定でした。 2004年の調査では、ダウンロードが音楽業界の収益全体に悪影響を及ぼさないことが示され[1457]、その後の調査では、ダウンローダーが実際に追加のCDを購入することが示されました[50]。  
 contentindustryは冷ややかだったが、その年の終わりまでに音楽出版社はAppleがオンライン音楽販売からの現金のシェアが多すぎることに抗議していた。  
 これは経済分析の予測力の印象的な実証です。  
 これについては、セクション24で詳しく説明します。  
DRMは2020年までに問題の問題がはるかに少なくなりました。リムーバブルメディアからストリーミングサービスへの移行は、音楽や映画をコピーする人がほとんどいないことを意味します。問題は、広告を回避するためにサブスクリプションを支払うかどうかです。  
 その結果、著作権侵害を含む犯罪が激減した[91]。  
 Googleドキュメントとの競合がOceの価格を下げる方法については上記で説明しました。そのため、MicrosoftはOcece365への移行で対応しました。そして、そのサービスまたはGスイートのいずれかの所有者シップの総コストが、スタンドアロンの生産性製品よりも高い方法です。6。  
 すべてのデータをいつでもダウンロードできますが、異なるプラットフォーム（MicrosoftやAppleなど）に再インストールするのは非常に面倒なので、無料の割り当てが実行されたときに歯を食いしばして、より多くのストレージを購入することになります。でる。  
 繰り返しますが、これは新しいことではありません。私の大学の恐ろしい会計システムは、約20年間、Oracle Financialsの大幅にカスタマイズされたバージョンです。  
Salesforceは多くの企業の販売管理を引き継ぎ、Palantirは多数の米国警察を拘束し、大手の学術出版社は大学図書館の機能を奪っています。  
 マイクロソフトロッキンの公共部門のITの深さは、ムーニッチ市がLinuxを離脱させて行政に使用しようとする勇敢な試みによって示されています。これは、15年後にビルゲイツを数回訪問し、新しい市長の後に最終的に取り消されました。 [759]。  
 大きなITサービス企業が市場の力を構築し、広告エコシステムからオペレーティングシステム、データセンターまですべてを制御する方法には、これの興味深い反響があります。  
 それが唯一の要因ではありません。他の産業（防衛請負など）には独自のダイナミクスがありますが、公益事業などの自然独占の規制当局は、ロビー活動によって時間をかけて捕らえられる傾向があります。  
 情報産業のダイナミクスは、これらの既存の問題の多くを悪化させ、効果的な競争をさらに困難にする可能性があります。  
 しかしカールは、過去40年間に米国の独占禁止法が最高裁判所によって過度に縮小されたことを認めている。消費者福祉テストが不十分であること。支配的な企業の排他的行動と労働市場の慣行の両方に取り組む必要があること、そして米国は水平合併をより適切に管理する必要があること[1717]。  
 ありそうな将来の方向性については、欧州委員会の総務安全工学のための2019年の報告287ロス・アンダーソン8。  
 Jacques Cr´emer、Yves-Alexandre de Montjoye、HeikeSchweizterによる競争の安全性と信頼性の経済学は、技術専攻のネットワークの外部性とスケールへの極端なリターンだけでなく、彼らが移動するデータのおかげでますます多くを制御しているという事実を強調していますオンラインサービスとクラウドコンピューティング[497]。  
 EUの競争法の枠組みは基本的には健全ですが、調整が必要であると結論付けています。規制当局は、市場での競争と支配的なプラットフォームなどの市場での競争の両方を保護する必要があり、そこでは競争を歪めない責任があります。  
スペアパーツの結束はヨーロッパでも規制されており、特定の法律では、ベンダーは他の企業に互換性のあるスペアパーツの製造を許可するよう要求しており、他のベンダーは一定期間スペアを利用可能にすることを要求しています。  
 これは、ソフトウェアコンポーネントの更新が利用可能になる期間をベンダーが制限する場合に、デジタルコンポーネントを備えた商品に対して強化される、計画的廃止に関する法律と関連しています。  
 そのような規制は、自動車や医療機器などの耐久財にソフトウェアが導入された今、さらに問題になるでしょう。この本の最後の章で持続可能性について説明します。  
6。  
•サイバー犯罪に対する警察の行動はほとんどありません。人々がそれを報告するのを阻止するのは簡単だからです。  
3、これにより、他のすべてのようにオンラインで移動しているだけであったにもかかわらず、犯罪が長年にわたって減少していると主張することができました。  
 しかし、どの銀行家も、顧客の1人がマフィオであることを本当に知りたがっていません。  
•詐欺に関しては、まれな銀行の詐欺パターンを発見することで、決済サービスプロバイダーは、顧客に誤解や嘘をついていることを伝えるだけでなく、損失を処理する必要があります。  
セキュリティエンジニアリング288ロスアンダーソン8。  
 セキュリティと信頼性の経済性•クリック詐欺も同様です。  
 最悪の事態を緩和するためにいくつかの作業を行う必要がありますが、市場での地位を独占している場合は、クリック詐欺に取り組むのが難しいほど、収益が少なくなります。  
 もちろん、動作を停止させる明らかなバグを微調整する必要がありますが、攻撃者が悪用できるより微妙なバグはどうですか？それらを探すために費やす時間が長いほど、それらを修正するために費やす必要がある時間が長くなります。そのため、企業は顧客がそれを要求する場合にのみそれを行う傾向があり、プロジェクトの最初からそれを行う場合にのみ安価です（ただし、その場合は、CではなくRustでコードを記述することもできます）。  
 取締役はインサイダーの脅威について取締役会と話すのは困難でした。そのため、典型的なセキュリティマネージャーは、内部統制を構築するための予算を確保するために、「悪質なハッカー」について恐ろしいプレゼンテーションを行います。  
 彼らが会社を倒さない限り、エグゼクティブ詐欺はめったに発見されません。代わりに、毎月パスワードを変更したり、元の紙の領収書を要求したりするなど、煩わしくて無関係な処理が行われます。  
2。  
または、セクション2で説明されている英国での2009年の議会支出スキャンダルを検討してください。  
6。  
 そのスローガンの作者、当時の内務長官であるジャッキー・スミスは、隠すことは何もなかったかもしれないが、彼女の夫はそうしました。彼はポルノを見て、議会の費用にそれを請求していました。  
 経費サーバーに関する情報が閣僚の仕事にかかる可能性があることを知っていた場合、おそらく彼らはそれをトップシークレットに分類して保管庫に保管しておくべきでした。  
8。  
6プライバシーの経済学プライバシーのパラドックスは、人々はプライバシーを大事にしているが、それ以外の行動はするということです。  
6。  
 ただし、オンラインとオフラインの両方でのショッピング行動はかなり異なります。大多数の人々はプライバシーにほとんど注意を払わず、ほとんどの利益のために最も機密性の高い情報を放棄します。  
 なぜこれが必要なのでしょうか？プライバシーは、関心のある経済学者が2000年以前に情報セキュリティの1つの側面であるということです。  
 1980年に、ジャックヒルスレイファーは、プライバシーを社会からの脱退というよりも、進化した領土行動から生じた社会を​​組織化する手段であると論じた独創的な論文を発表しました。内在化されたプロパティの尊重はオートトノミーをサポートします。  
 消費者は無関係なマーケティングコールに悩まされたくない一方、マーケティング担当者は無駄を省きたいです。それでも、検索コスト、外部性、その他の要因のため、どちらも苛立たしいものです。  
ただし、これまで見てきたように、情報産業は独占につながる市場の失敗に陥りやすく、支配的で情報集約的なビジネスモデルの急増には異なるアプローチが必要です。  
 企業は個人の支払い意欲を明らかにするデータを求めてオンラインインタラクションをマイニングします。航空会社の歩留まり管理システムから通信料金まで、多くの市場で見られる差額料金は経済的に効率的かもしれませんが、ますます不満を抱いています。  
 テレセールス事業者が100人の見込み客に電話をかけ、3つの保険を販売し、80を困らせる場合、従来の経済分析は3人と保険会社の利益のみを考慮します。  
 ロボコールの長期的な社会的コストはかなりのものになる可能性があります。  
プライバシーのパラドックスは重要な文献を生み出し、少なくとも3つの要因が加わっています。  
次に、セクション3で説明した行動要因。  
5はより大きい役割を果たします。  
 彼女は恥ずかしい質問のリストという形で「プライバシーメーター」を考案しました。スコアは、被験者が怒鳴る前に回答する質問の数でした。  
笑顔の悪魔のロゴが入ったcom）。  
 ゲーマーグループに関しては、彼らは幸福にもセキュリティエンジニアリング290ロスアンダーソン8です。  
 セキュリティと依存性の経済学は、対照群の2倍の量を開示しました[987]。  
 プライバシーポリシーは通常、トップページにはありませんが、関係するユーザーが簡単に見つけることができます。通常、ポリシーはanodyneテキストで始まり、不愉快なstu theを最後まで残します。そのため、カジュアルな視聴者に警告することはありませんが、注意深い少数派は、サイトを使用しない理由をすばやく見つけることができるため、他のユーザーのクリックを阻止しません。広告。  
2。  
では、全体的な効果は何ですか？ 2000年代と2010年代初頭には、リスクについて私たちエンジニアがすでに理解していることを一般の人々が徐々に学んでいるという証拠がありました。たとえば、プライバシーコントロールを使用してシステムの非常にオープンなデフォルトを狭めることを選択するFacebookユーザーの割合が着実に増加していることで、これを見ることができます。  
 成人の93％は、自分に関する情報を誰が入手できるかを管理することが重要であり、90％が彼らについて収集される情報を管理することが重要であると述べました。 88％は、誰も許可なしに視聴しないようにすることが重要だと述べています。’電話会社とクレジットカード会社の数字は似ていましたが、広告主、ソーシャルメディア、検索エンジンの数字は著しく悪化していました。  
これらの緊張は1960年代以降高まっており、米国とヨーロッパの間で著しく異なる複雑なプライバシー規制につながっています。  
6。  
6。  
 企業や政府でさえも非常に自己満足的になり、パニックに陥る危機になるまで、脅威に対処することができなくなることがよくあります。  
 別の例として、悪意のある人たちが狙っている電話会社と銀行は常に1つあるようです。  
 虐待の波の高まりは、可能な限り無視され、または顧客に非難されます。  
 大量のお金が1〜2年費やされ、stu↵が修正され、悪者が次の犠牲者に移動します。  
セキュリティエンジニアリング291ロスアンダーソン8。  
 セキュリティと信頼性の経済学トルスタインヴェブレンに遡る制度経済学に関する重要な文献があります。  
 管理行動に関する古典的な本で、彼はマネージャーが下す決定は効率性だけでなく組織の忠誠心と権威、そして組織の目標と個々の従業員が直面するインセンティブの間の相互作用であると説明しました。目的の複雑な階層があり、値と事実は混同されています[1754]。  
 会計の実際の実践の失敗については、後でセクション12で説明します。  
 もう1つのアプローチは、公選経済学です。これは、ミクロ経済的手法を使用して、政治家、公務員、および公的機関の人々の行動を一般的に研究します。  
3。  
 Cynicsは、官僚主義は非難の可能性を最小限に抑えるような方法で進化しているように見えると指摘しています。  
 大学の教授たちは互いに懸命に競争している。私たちの顧客は私たちの副首相ではなく、ノーベル賞委員会または同等のものです。  
 一方、一部の民間企業は、内部で政府と同じように振る舞うほどの市場力を持っています（ただし、給与ははるかに優れています）。  
6。  
 これにより、サイバー犯罪の経済学がもたらされます。  
3サイバー犯罪のエコシステムの概要を説明しましたが、より詳細に調査するために使用できる多くのツールがあります。  
他の経済分野と同様に、興味深い質問とは何かを考え出し、それに答えるためにデータを収集するという反復的なプロセスがあります。  
犯罪へのアプローチの1つは、1968年に報酬と罰の観点から犯罪を分析したGaryBeckerなどのシカゴ学校の経済学者のアプローチです[200]。  
 犯罪が悪い地域に集まっているのはなぜですか？なぜこれらの近所の子供たちが多産で執拗な放浪者になるのでしょうか？従来の犯罪学者はこのような質問を調査し、犯罪防止における価値の説明を見つけます。最悪の犯罪者は、多くの場合、子育てが不十分で、薬物乱用や薬物乱用など、複数の剥奪に悩まされ、犯罪のサイクルに引き込まれます。  
6。  
 犯罪統計学者は、法律は貧しい人々を抑圧することによって彼らの力を維持する強力な人々によって作られていること、そして悪い地域は裕福な白人が住んでいる素敵な郊外よりも過度に厳しく非難される可能性が高いと指摘しています。  
 1960年代以降、犯罪を抑制するために環境設計を使用することについて、最初は低コストの住宅で、その後あらゆる場所で、かなりの量の研究が行われてきました。  
 セクション13。  
2これについて詳しく説明します。  
 銀行強盗は銀行家を本当の搾取者として見る。兵士は敵を「グーク」または「恐怖」として非人間化します。そして、最も一般的な殺人者は彼らの犯罪を名誉の問題と見なしています。  
2。  
これらのメカニズムは、オンラインおよび電子詐欺の世界にまで及んでいます。  
 一部のロシアのサイバー犯罪者は、米国が1989年以降にロシアを台無しにしたとの見方をしているので、彼らは彼ら自身を取り戻しているだけです（そして、彼らはこれで彼ら自身の政府の態度と政策によって支持されます）。  
第三に、犯罪への道、犯罪集団の組織化、スキルの拡散を理解することが重要です。  
 彼らは雨の中で立ち、次のレベルに上がるチャンスのために撃たれる準備ができていました、そこで近所のボスは3人の女の子と一緒にBMWで駆け回りました。  
 結果を得るために、警察は輸入業者のシステム管理者などのチョークポイントをターゲットにする必要があります。多くのサイバー犯罪者はゲーマーとして始まり、その後ゲームをだまし、ゲームの攻略を扱い、その後ゲームの攻略をコーディングする方法を学び、数年以内に才能のある人がマルウェア開発者になります。  
 セクション3で述べたように。  
4、英国国家犯罪庁はGoogleの広告を購入し、英国の人々がDDoS-for-hireサービスを検索しているときに、そのようなサービスの利用が違法であることを警告しています。  
セクション2でサイバー犯罪の全体的なコストについて説明しました。  
7。  
 現在、ほとんどの買収犯罪はオンラインです。 2019年には、約100万の英国世帯が強盗や車の盗難に遭遇し、200万世帯以上がほぼ常にオンラインで詐欺や詐欺に遭遇すると予測しています。  
）イエットポリシーの対応はほとんどどこでも遅れています。  
サイバー犯罪の影響は、漏えいの開示の影響によっても調査されます。  
 違反の開示に関する法律は、違反を保険にかけられない出来事にしています。 TJXが4700万件のレコードを失い、各顧客に郵送するために5ドルを支払う必要がある場合、それはクレームです。サイバー保険については、後のセクション28で説明します。  
9。  
 関連する出版物のほとんどは、警察機関からウイルス対策ベンダーまで、損失について話し合うインセンティブを持つ組織からのものです。セクション2に示すように、推奨される方法は、手口とセクターごとに損失をカウントすることです。  
8。  
 その結果、セキュリティエンジニアは、基本的な経済学だけでなく、暗号、プロトコル、アクセス制御、心理学の基本を理解する必要があります。  
 それは、人々が本当にプライバシーを気にするかどうかを通してパッチ適用サイクルを最適化する方法からあらゆる種類の質問への魅力的な新しい洞察を常に投げ出します。  
 経済学は広大な主題です。  
 最初に、セキュリティと、経済学の他のサブフィールドXについて考えます。  
第三に、金を見つけたら、掘り続けます（e。  
 行動プライバシー）[78]。  
第4に、セキュリティエンジニアリング294ロスアンダーソン8を始めた今、データ主導の研究には多くの余地があります。  
 （Cambridge Cyber​​crimeCentreを介して）大規模なデータセットを学者が利用できるようにするために、多くの学生がデータサイエンスのスキルの開発に熱心です。  
 セキュリティ文化の質を測定する良い方法はありますか？第5に、自動車や医療機器などの安全性に不可欠なソフトウェアやオンライン接続を導入し始めています。セキュリティと安全性の相互作用について、そしてこのようなシステムにパッチを適用して何十年も実行し続ける方法について、多くのことを知る必要があります。 。  
セキュリティ経済学に関する現在の研究は、主に2002年から毎年開催されている情報セキュリティの経済学（WEIS）に関するワークショップで公開されています[76]。  
cl。  
交流。  
html。  
 これはまだ生徒の読書リストにあります。  
Tim Wuの「The Master Switch」は、10年前の観点から、通信および情報産業における独占について概説しています[2049]。  
 アダム・スミスの古典的な「国々の富と自然の原因についての探究」は一見の価値がありますが、ディックターラーの「不作法」は行動経済学の物語です。  
 プライバシーの経済性については、Alessandro Acquistiのオンライン書誌と、George LoewensteinとLaura Brandimarteによって彼が書いた調査論文[16]を参照してください。 Spiros Kokolakisによるプライバシーパラドックスに関する文学の調査もあります[1076]。  
多くの経済学者が関連分野を研究しています。  
 Diego Gambettaは、おそらくSecurity Engineering295Ross Anderson8です。  
 概要組織犯罪の第一人者;彼の「アンダーワールドのコード：犯罪者とのコミュニケーション方法」は古典的です[742]。  
セキュリティエンジニアリング296ロスアンダーソン