それ以来、いくつかの大きな変化がありました。  
現在、世界のほとんどの人口は、電話、カメラ、衛星ナビゲーションを兼ねたコンピュータを持って歩き回っています。そして、これらの魔法のデバイスで実行されるアプリは、10年前に私たちが構築していたものの多くを置き換えました。  
銀行業務は主にオンラインになり、電話はクレジットカードに置き換わり始めています。  
ソーシャルネットワーキングは多くの人々の生活を引き継ぎ、広告から政治まですべてを推進しています。  
機密データは、学校、医師のオフィス、法律事務所のサーバーからクラウドサービスプロバイダーに移行しています。  
。  
セキュリティ侵害は、20年前に誰も想像もしなかったような規模で発生する可能性があります。  
そして2013年に、患者の同意なしに、15年間分の英国の病院の医療記録が世界中の1200の組織に販売されていたことを発見しました（患者は郵便番号と生年月日によって識別可能でした）  
過去10年間で最大の変革者はおそらくスノーデンの改定であり、2013年にもNSAの信号インテリジェンス活動に関する50,000を超えるトップシークレットの文書が報道機関に漏らされました。  
これにより、3番目の大きな変化がもたらされます。これは、セキュリティの脅威をよりよく理解するためです。  
そして、お金がどこにあるのか、詐欺師も追随します。  
ケンブリッジにはこれを研究するチームがあり、世界中の他の何十もの研究者グループもそうです。  
そして、ネットいじめなどの個別の脅威があり、通常は刑事訴追のしきい値を下回りますが、本当の苦痛を引き起こし、ソーシャルネットワークによって容易になり、問題となるほどの規模で発生します。  
これらの害のコストと、それらを軽減するために導入する対策の有効性を測定することはこれまで以上に重要です。  
たとえば、40年以上にわたって米国政府が数十億ドルの資金を提供してきたにもかかわらず、マルチレベルのセキュリティ業界は瀕死の状態にあります。国防総省の情報セキュリティ哲学全体、つまり、トップシークレットからシークレット、コンフィデンシャル、未分類へと流れる情報を停止するように強制するアーキテクチャーは、機能しないとして放棄されました。  
バグは至る所に存在し、エクスプロイトは避けられないため、エクスプロイトの検出、バグの修正、および攻撃からの回復が得意です。  
将来はどうなるのでしょうか？  
これは本当の緊張につながります。セキュリティエンジニアはすぐにバグを修正しますが、安全エンジニアは、ゆっくりと変化する規格に対してシステムを厳密にテストすることを好みます。  
現時点では、3年間は携帯電話用のセキュリティパッチを、5年間はノートパソコン用のセキュリティパッチを入手できます。その後、新しいものを購入する必要があります。  
では、2022年に発売される自動車向けのナビゲーションソフトウェアを今日作成している場合、2032、2042、2052でセキュリティパッチの出荷を継続できるようにするために、どのツールチェーンを選択しますか？  
政治指導者がテクノロジー政策をアノラックのためのものであると見なし、一般に抵抗が最も少ない線をとった数十年後、ブレグジット国民投票とトランプ選挙へのロシアの干渉の報告は本当に注目を集めました。  
議員の細心の注意がゲームを変えることであり、まずはより厳しい規則（ヨーロッパの一般データ保護規則など）で  
セキュリティエンジニアが今日尋ねなければならない質問は、10年前と同じです。何を防止しようとしているか、提案されたメカニズムは実際に機能するでしょうか。  
ほとんどすべての人間の生活はそこにあります。