Q What is "zero trust" in information security? Is it a new concept or just old wine in a new bottle?

A I will start with an anecdote. When I started my IS audit career after earning the Certified Information Systems Auditor® (CISA®) certification, most organizations had implemented risk management that was limited to business risk, and technology risk was left to be managed by chief information officers (CIOs). During audit meetings, when I would discuss findings that demonstrated weak controls, the most common response from CIOs would be, "But we trust our employees, so such stringent controls are not required. They may affect the efficiency of service delivery." I always endeavored to respond with a positive: "I agree with you, all your employees are excellent. However, your controls must be forward looking. In several years, when most of your current employees retire or move to other jobs, will these current controls operate with the same trust levels?" Most CIOs would then agree that trust must be disregarded and the controls implemented. In general, organizations tend to trust insiders, that is, authorized users, and do not trust outsiders. Zero trust starts with treating insiders and outsiders at par.

This brings us to the second part of the question: Is zero trust old wine in a new bottle? The simple answer is it is a basic concept in risk management that has been revised with enhanced scope so as to implement it while deploying infrastructure, resources and, hence, security.

In risk management, we learn that "Trust is anathema for risk mitigation," or, to put it another way, although you may decide to trust resources used, do not consider that when designing controls to mitigate risk. However, many times we go for the easier, faster route and overlook this principle.

To put it simply, zero trust means designing and implementing controls for mitigating risk without trusting the resources (i.e., people, processes, technology) deployed. Why it is being considered now? Current changes in technology deployment, advances in automation and the global pandemic have highlighted the need for considering zero trust. Many organizations are considering a move or have already moved to cloud. Federated identity management or identity management as service are being seriously considered. The use of emerging technologies such as robotic process automation (RPA), artificial intelligence (AI) and the Internet of Things (IoT) have been on the rise. In such a rapidly changing tech climate, it is necessary to rethink the traditional castle-and-moat security approach focused on the perimeter.

The coronavirus pandemic created additional challenges for security managers. During the pandemic-induced lockdown initiated in many countries, organizations had to resort to work-from-home (WFH) employment models. Many organizations were not prepared and had to resort to immediately available, quick solutions that included allowing users to use their own devices and home networks to connect and access the organization's resources. The question became "Can we trust these home networks and devices to be secured as per the organization's requirements?" This prompted security managers to consider controls without trusting the resources.

To implement zero trust, organizations can consider deploying technologies such as multifactor authentication (MFA), identity and access management (IAM), orchestration, data analytics, encryption, score cards, and performance monitoring and file system permissions. Zero trust requires the governance of policies such as giving users the least amount of access required to accomplish a specific task. Zero trust does not eliminate trust completely, but it is about using technologies to enforce the principle that no user and no resource has access until it has been proven they can and should be trusted.

Like all other security implementations, zero trust requires ongoing effort. However, zero trust must be built by design, not by retrofit. Zero trust should involve C-suite executives, the chief information security officer (CISO), the CIO and others to determine priorities and ensure that it will be implemented across the organization.

Going forward, many organizations have already accepted that there will be a new normal for conducting operations in a post-pandemic world. The zero trust model for enterprise architecture, information security and governance will be part of this new normal.

Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP
Has worked in IT, IT governance, IS audit, information security and IT risk management. He has 40 years of experience in various positions in different industries. Currently, he is a freelance consultant in India.

> “ZERO TRUST IS IT IS BASIC CONCEPT IN RISK MANAGEMENT THAT HAS BEEN REVISED WITH ENHANCED SCOPE SO AS TO IMPLEMENT IT WHILE DEPLOYING INFRASTRUCTURE, RESOURCES AND, HENCE, SECURITY.”

Q What is the “right to forget” in privacy compliance? Will it override the regulator-specified compliance requirements for data retention, particularly for my organization that operates in the banking industry sector?

A Privacy is a powerful right that allows any individual to decide how their personal information can be used by an organization, which is collecting such personal information or which can transfer that information to other parties for the purpose of further processing. When any organization collects personal information from its data subjects (e.g., employees, customers, vendors, independent contractors) to provide better services, often the organization collects personal information that may not be required. Organizations must stick to the privacy principle of data minimization. Most privacy regulations focus on regulating organizations while they are collecting, storing, communicating, securing, sharing/transferring/disclosing and disseminating information so collected. For this, organizations need a robust privacy governance program.

The EU General Data Protection Regulation (GDPR) has become the *de facto* standard due to its comprehensive nature. GDPR is the first regulation that provided the right to be forgotten or the right to erasure to the data owner (data subject). This right gives the data owner the ability to direct the organization that has collected the personal data to erase such data once the required service relationship is over.[1] Note that this is not an absolute right in the hands of data subjects. There are certain exceptions where it supports organizations such as banks to comply with the requirements of other applicable laws. In other words, a customer of a bank may request that a bank erase all the customer’s personal data after closing an account or terminating the relationship. Article 17 of GDPR has outlined the possible situations where the exceptions to this right may not be applicable to the organization collecting personal data (data controller).[2] One of the situations described under Article 17 addresses the legal and regulatory compliance requirements by the organization. Other exceptions where organizations may not comply with the right to be forgotten when data need to be retained are:

- For exercising the right of freedom of expression and information
- For the performance of a task carried out in the public interest (explained in other articles of the regulation)
- For exercising official authority vested in the organization as data controller
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, or if removal of the data would seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defense of legal claims (litigation hold)

It is important for banks to clearly highlight such exceptions in their privacy notice provided to the public at large on their websites. Further, organizations may need to communicate these exceptions to data subjects when data subjects raise their right to be forgotten through the Data Subject Rights request portal and give a reference to the privacy notice given at the time of collecting the personal information.

There are two good solutions for protecting databases containing personal information:

1. An organization can encrypt the entire database with strong encryption keys and algorithms and make it such that access to the database is provided on a need-to-know basis only.
2. It is good practice to use anonymization of personal data while retaining data for any of the reasons stated herein. This helps to protect against the accidental leakage of personal data. It also helps to achieve the required purpose of data retention, and personal information may be accessed only when it is required.

Endnotes

[1] Intersoft Consulting, Art. 17 GDPR, Right to Erasure (“Right to Be Forgotten”), Belgium, 2018, *https://gdpr-info.eu/art-17-gdpr/*

[2] *Ibid*.