In the IT and cybersecurity realms, change is inevitable. Digital advancements fuel innovative ways of doing things, spawn new industries and radically transform how people interact on a global scale. As one of ISACA's newest board directors, it is encouraging to see how the association's professional community influences the development of technologies, modern standards, effective governance models and best practices that drive positive change in the public and private sectors.

Moving Beyond Compliance

Traditional governance models are built on compliance-based governance models. Most executives do not want to spend any more than they have to for IT and cybersecurity capabilities, yet they are sensitive about being compliant with regulatory standards.

The time has come to move beyond traditional compliance, as the rate of change in today's technology-reliant environment outstrips the ability of regulators to keep standards current. Compliance will not necessarily bring an enterprise best practices, but implementing best practices will bring it compliance. Leading organizations have accepted that compliance is the baseline and best practices are the must-reach goal.

People, Processes and Technology: Separate, but Equal Elements

When it comes to digital transformation efforts, too many people chase fads rather than implement well-designed, choreographed plans that foster business imperatives, such as improvements in business operations, profitability, customer experience, security and efficiency. The rush to insert the latest and greatest technologies often falls flat and results in underperforming organizations, unhappy customers and/or skeptical boards unwilling to reinvest further in speculative transformation efforts.

Digital transformation efforts fail or underperform when they make technology the sole focus. Initiatives are doomed if an organization does not transform people to properly operate and maintain the equipment and/or fails to change processes to best leverage the technology.

Do Not Eliminate Risk. Manage It.

As people, processes and technology are equally important factors in managing risk, leading organizations keep a strong focus on all three. Potential adversaries do as well.

Gregory J. Touhill, CISM, CISSP

Is a retired US Air Force Brigadier General and current president of the Cyxtera Federal Group, which offers market-leading data center services and cybersecurity capabilities to US federal agencies and departments via a portfolio of secure infrastructure solutions delivered from a global footprint of world-class data centers, including six in the Washington DC, USA, metropolitan area. Prior to joining Cyxtera, Touhill was appointed by US President Barack Obama as the nation's first-ever federal chief information security officer in 2016, where he was responsible for ensuring that the proper set of digital security policies, strategies and practices were adopted across all US government agencies. He can be reached at https://twitter.com/cyxtera and https://www.linkedin.com/in/gregorytouhill/.
Hackers, cybercriminals and rogue nation-states know that if an attack is to be launched, all three must be taken into consideration. Therefore, a more holistic view of risk exposure is required.

Fortunately, today's workforce is increasingly cyber aware. Organizations and individuals are making investments in advanced education and mentoring programs, recruiters are requiring specialty certifications, and there is a greater emphasis on retention and succession planning.

For example, the US government launched an initiative to grow a more capable cyber workforce by promoting employees earning cyber certifications such as ISACA's Certified Information Security Manager® (CISM®) and Certified Information Systems Auditor® (CISA®) credentials. In many organizations, cyber professionals who earn and maintain current certifications receive special pay. A well-trained and focused cyber workforce reduces cyber risk.

While there has been momentum toward "hardening the workforce," there is a way to go to improve processes. Organizations rarely address transforming business processes in concert with the insertion of new technology. An organization with the latest technology, but sporting antiquated processes, is like sitting behind the wheel of a high-performance car while stuck in a holiday traffic jam.

Effective governance models ensure that process transformation is part of the checklist guiding not only the digital transformation effort, but also the daily management and oversight of operations. More Certified in the Governance of Enterprise IT® (CGEIT®) professionals are needed to help champion process improvements that accelerate and improve digital transformations in every critical infrastructure sector.

**Time to Retire Antiquated Infrastructure**

Several years ago, inspired by the famous Moore's Law, I created Touhill's Law: One human year equals 25 computer years. Here is the three-factor logic behind it.

First, there is a common adage about calculating a dog's life span: One human year equals seven dog years. Secondly, great technology companies such as Microsoft, Apple and Google (typically) come out with a generational product every three years. Third, government agencies estimate the average life span of a human at around 75 years. Dividing three years (measure of a computer generation) into 75 (measure of a human life span) produces a result of 25. Therefore, one human year equals 25 computer years.

Touhill's Law reinforces the fact that an aging infrastructure is risky. While serving as the US government's chief information security officer (CISO), I found that the US government operates numerous computers that are (effectively) hundreds of years old, frail and difficult to sustain, expensive to operate, and highly vulnerable to malfunction or exploitation by hostile forces. (One computer was discovered that came online in 1964!)

Like employees whose training is not current, and processes that are no longer effective, antiquated infrastructure (including architectures, software, hardware and communications) needs to be continually assessed for retirement. With today's digital transformation already underway and accelerating, now is the time to make prudent investment and recapitalization decisions that will enhance performance, improve security and reduce overall costs.

Unfortunately, many organizations still use 1990s technology and architectures (e.g., virtual private networks [VPNs], firewalls, individual encrypted links for every communication, network access controls [NACs]), which have become porous "barrier reefs." Multiple breaches over the past 20 years have proven that hostile adversaries easily find the holes and sail right through them to hit their targets, while task-saturated IT professionals labor to continue to keep their increasingly complex, Frankenstein-like environments up and operating.

VPNs and firewalls celebrated their 22nd birthdays this year. For those counting, that is 550 years, according to Touhill's Law. Clearly, it is time to transition to a more modern, secure infrastructure that protects national prosperity and security.

When assessing risk and refining governance models, it is critical to remain cognizant that architecture is a key ingredient in delivering results that are effective,
efficient and secure. Architectural information should be treated as high-priority information worthy of protection at the same level as the most valuable information contained in the network.

Marking Time Means Falling Behind

Transforming access controls with effective 21st century technologies, such as software defined perimeter (SDP) technology that obviates the need for VPNs and is capable of securing any application, on any platform, in any location, is imperative.

SDP is identity-centric and addresses a critical weakness in the Transmission Control Protocol (TCP)/Internet Protocol (IP), which connects then authenticates users. This weakness is risky as malicious actors can gain access to devices without ever having to authenticate. SDP defeats this vulnerability by authenticating first before connecting to only what the user is authorized to access. SDPs operating at layer three in the Open Systems Interconnection (OSI) model are best because latency is minimal when running at the network layer.

SDP enforces the “zero trust model” by applying the principle of least privilege to the entire network, a huge advantage for network defenders. SDP is built for the cloud and is like the cloud, so it operates natively in cloud networks, is completely distributed and is as scalable as the Internet itself.

Be Careful Flying Into the Clouds

During 30 years in the US Air Force, I learned that a pilot should never fly into a cloud without knowing what is inside. Migrating legacy infrastructures into cloud-based environments is a key component of contemporary digital transformations, yet such migration is fraught with risk for those who do not do their homework.

As a former chief information officer (CIO), I am a huge fan of cloud technology. The benefits are many, including faster infrastructure provisioning, lower total cost of ownership and elasticity. In addition to the need to implement SDP in cloud environments, here are some recommendations for CIOs that will enhance cloud migration and operations:

- **Include a portability clause in every cloud vendor services contract.** A CIO must be prepared to move data from one place to another at the conclusion of a contract. It is necessary to be able to not only move data to a new provider, but also ensure that the data are properly disposed of on the first cloud provider’s infrastructure at the conclusion of the engagement.

- **Require unfettered access to logs and review them regularly.** Logging and reviewing network traffic is an essential element of first-class cybersecurity programs and helps network defenders identify when their network is out of parameters or under attack. They are due care and due diligence practices. When moving to the cloud, ensuring access to and reviewing logs applicable to the enterprise’s data are essential, as is running independent analytics to stay ahead of potential internal and/or external threats.

- **Retain the right to conduct penetration testing.** Testing defenses identifies how secure (or insecure) a network is and pinpoints best practices and areas for improvement. CISOs should ensure that the right to penetration test is included in their cloud requirements as well as the final contract.

- **Retain the right to conduct an independent third-party audit to ensure contract provisions are being properly provided.** If the organization flies into the cloud without knowing what is in it, chances are the organization has no idea if it is getting what it paid for or if its data are at risk. Hiring an expert with the business and technical skills to audit the relationship, people, processes and technology involved on all ends pays dividends to avoid a worst-case breach scenario.

The ISACA community knows that modern enterprise IT is diverse, dynamic and distributed. It is time for ISACA professionals to help organizations embrace digital transformation and deliver results that are more effective, efficient and secure. The world’s economic prosperity and security depend on it.

Endnotes

1 Moore’s Law, www.mooreslaw.org/