In this time of the COVID-19 pandemic, personal cleanliness and hygiene are discussed more frequently than ever before. It is essential to maintain hygiene to stay safe and prevent the spread of COVID-19. Even from a cost perspective, the cost of being cautious is lower than the cost associated with COVID-19 infection and the psychological costs. The root of hygiene is discipline. It drives maintaining hygiene. Good hygiene is everyone's responsibility to protect themselves and the community.

How does this relate to IT or IT security? If every employee is disciplined in understanding and maintaining secure IT functions and security hygiene, many IT security issues would never occur. For example, employees should understand all of the following concepts to maintain IT security hygiene:

- Use of strong passwords
- Not sharing passwords with anyone
- Not leaving their personal laptop or desktop without locking it
- Use of the facility (i.e., workplace) only for the purpose provided
- Not using enterprise-provided devices for personal purposes
- Avoiding inappropriate websites
- Not installing unapproved software on any work-related device
- Not allowing unauthorized users to access enterprise devices
- Using the most recent security software versions
- Not allowing piggy backing while accessing facilities. Piggy backing refers to when a person tags along with another person who is authorized to gain entry into a restricted area or passed a certain checkpoint. It can be either electronic or physical. There would be no record for the person's entry into the facility, which creates a security issue.

Security hygiene means:

- Focus on the basics (e.g., timely patching, moving away from unsupported versions).
- Security resources are scarce and limited, so security implementation should be prioritized based on business criticality.
- There are numerous security solutions and services available in the market. Choose security
products and services based on the business scenario. There is no one-size-fits-all solution.

* Perform security assessments and actions based on the organization's current state. For example, some vulnerabilities may be rated high risk, but the scenario may not be applicable to the organization. On the other hand, there are some vulnerabilities that may be rated medium or low risk in the market but would be high priorities for the organization.

* In this new age of digitalization and business advancement, security teams should engage seamlessly with the business to enable the release of products and services without compromising security.

One way to understand IT security hygiene is to use a bottom-up approach based on the seven layers of security as well as a top-down approach from the leadership perspective.

Per the Open System Interconnection (OSI), as developed by the International Organization for Standardization (ISO), any IT system should have seven layers of security architecture, with each layer having a specific functionality to perform. All seven layers work collaboratively to transmit data from one person to another across the globe.

Security Rule Book: Information Security Policy

For any organization to be successful in establishing security, it should have an information security policy (ISP) to ensure the foundation of security and the appropriate use of resources.

In the complex world of IT, classifying information by the ISO OSI model could be the starting point. As previously stated, there are seven layers of architecture that split the communication system into abstraction layers. For example, a layer that provides error-free communications across a network provides the path needed by applications in layers above it, while it calls the next layer to send and receive packets that constitute the contents of that path.

"FOR ANY ORGANIZATION TO BE SUCCESSFUL IN ESTABLISHING SECURITY, IT SHOULD HAVE AN INFORMATION SECURITY POLICY (ISP) TO ENSURE THE FOUNDATION OF SECURITY AND THE APPROPRIATE USE OF RESOURCES."

Understanding the OSI model helps in understanding the seven layers of security:

1. **Physical**—This is the lowest level of security. At this layer, systems are locked to keep them safe (e.g., adding physical access restrictions for workstations, restricting access to data centers, restricting access to racks where servers are kept). Having strong security measures implemented at this layer can eliminate issues such as direct wiretapping, signal jamming, tailgating and unauthorized access.

2. **Data link**—At this layer, data are moved from software to hardware and back. Security at this layer keeps data moving to where they are supposed to go.

3. **Network**—This layer is also called the Internet layer, as it connects different networks. Security at this layer protects attackers from accessing logins and passwords sent over the network, prevents flooding attacks, and prevents sniffing/snooping attacks.

4. **Transport**—This layer predominantly transports the workload from point A to point B and makes sure it is delivered securely and without any alteration. Strong security implementation at this layer could avoid denial of service (DoS) and man-in-the-middle (MitM) attacks.

5. **Session**—The session layer provides the mechanism for opening, closing and managing a session between end user application processes (i.e., a semi-permanent dialog). It adds synchronization points or checkpoints in data streams for long communications. Success of security at this layer means prevention of attacks such as DoS and spoofing.
6. Presentation—The presentation layer is responsible for presenting the data to the application layer. This may include some form of format or character translation.

7. Application—This layer is the closest to the end users. Some examples are web browsers and email clients. Securing this layer means preventing browser hijacking or spam outbursts.

Each of the layers are vulnerable to direct and indirect attacks. The layers must be continuously monitored and adjusted so the ecosystem is protected, the attack surface is minimized and business runs as usual. Even if the security of one of the layers is compromised, it could destabilize and render the entire ecosystem insecure. Adhering to IT security hygiene could ensure the elimination/avoidance of weakness, which can result in solid foundational security for the organization.

IT ISP
An ISP identifies the rules and procedures for all individuals accessing and using an organization's IT assets and resources. The objectives of an ISP are preservation of the confidentiality, integrity and availability of systems and information used by an organization's members.

To successfully adopt an ISP the policy should:
- Be simple to understand. Policies need to be stated in a way that the audience can understand, and they need to reflect and convey the reason the policies exist.
- Be enforceable, but flexible. Policies should be broad enough to be able to achieve common understanding across technologies.
- Be measurable in a consistent manner
- Minimize unintended consequences

An information security framework consists of a number of documents that clearly define the adopted policies, procedures and processes by which an organization abides. It effectively explains to all parties (i.e., internal, tangential, external) how information, systems and services are managed within the organization.

For an organization to demonstrate it is secure, it needs to have a solid ISP derived from a recommended framework as deemed fit with respect to the organization.

Some examples of popular ISP frameworks include:
- Payment Card Industry Data Security Standard (PCI DSS)—A set of requirements intended to ensure that all organizations that process, store or transmit credit card information maintain a secure environment
- Center for Internet Security (CIS) Critical Security Controls—This is a list of 20 actions designed to mitigate the threat of the majority of common cyberattacks. The controls were designed by a group of volunteer experts from a range of fields, including cyberanalysts, consultants, academics and auditors.
- US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Security—This is a voluntary framework primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on existing standards, guidelines and practices.

People, Processes and Technology
It is helpful to view IT security hygiene with respect to people, processes and technology (figure 1).

People
Security is incomplete without “u.” Security is every employee's responsibility, regardless of whether said employee is full time or part time, a contractor or in a leadership position, IT or non-IT, or works on the shop floor or at corporate headquarters. Every employee of an enterprise must be disciplined in following their job responsibilities, thereby ensuring hygiene in their physical and virtual workplace environment. Untrained employees can be the weakest link in the chain. All it takes is for one employee to inadvertently click on an attachment of a malicious email, allowing attackers to take advantage of the enterprise. Proper training,
frequent communication and surprise evaluations can help employees to be vigilant. In short, it is the responsibility of each of the employees, which includes the leadership team, line managers and all other employees in the team structure of the organization (figure 2), to know of and abide by security policies mandated by the organization.

Managers
Middle managers are in positions to interface between employees and leadership. The manager is tasked with ensuring that employees develop the skills needed to maintain, sustain and propagate good hygiene. They play a crucial role in enforcing objectives and expectations and act as a bridge to help keep employees in alignment with management expectations. It is crucial to identify the most suitable person for these positions.

Because managers have a certain amount of authority in making day-to-day decisions, they have direct impact on the day-to-day functioning of enterprise operations. In short, managers are responsible for their teams adhering to the security mandates without any let up.

Leadership
C-suite personnel and leadership are directly responsible and accountable for the overall well-being of the organization and its employees. The phrase “tone at the top” refers to the leadership’s take on a variety of things. For security, it is very crucial that any actions align with leadership objectives. If the leadership team is portraying confidence and support of IT actions, it will automatically mean the message resonates further into the ranks of employees and departments.

It is not enough to formulate a policy and approve it. It is how the policy is implemented and the value it delivers that determines the success of its intent.

For example, during an audit, there is a condition that is flagged as a major comment by the auditor. The product line manager then involves the leadership and other required stakeholders in this particular vertical to assess the impact, assess the time needed to fix the condition and ensure the sustenance of the controls implemented.

Management should encourage employees when employees alert them to issues and guide employees to use this experience so that issues are identified and can be addressed. This will motivate employees to be vigilant in looking for any opportunities to eliminate security concerns in the future.

Employees should be motivated to bring security issues to the attention of management. There should never be a situation where employees are afraid to do so, as it would be counterproductive.

The seriousness and importance of leadership to the discipline and hygiene of the organization is directly reflected in their buy-in and requires support from the
employees. For any major security gaps, an organization's culture is reflected in the presence of leadership in the related discussions. It is much easier to ensure proper security measures that comply with leadership objectives and regulations in the first place rather than trying to fix things retroactively.

At the end of the day, if there are any issues, concerns or violation of processes, leadership stakeholders are directly accountable. In some situations, they could be legally liable and punished by court of law. Take, for example, the accounting scandal of US energy, commodities and services enterprise Enron Corporation and the dissolution of Arthur Andersen LLP, which had been one of the largest auditing and accounting enterprises in the world in 2000. Enron's estimated losses totaled around US$74 billion and the chief executive officer of Enron was convicted of federal felony charges and sentenced to prison.³

It may be a struggle for non-IT professionals in an enterprise to understand IT terminology, risk and complexities. At a security summit, there was a skit about delivery at market speed. There was a product built for public use that needed to be deployed in a couple of hours. However, the required security evaluations were not conducted, as the security team was separate and was only to be involved once development teams engaged it to verify security. In this scenario, the enterprise wanted to release the product for consumer use, but the security team was against it and was asking for time to evaluate the security of the product. The security team asked enterprise leadership to fill out a form to understand the risk and sign the document as part of “risk acceptance.” For enterprises, this risk acceptance may seem simple, as it removes the obstructions to rolling out the product, but many times the document is signed without understanding the depth of the risk and its implications. The skit then demonstrated a better solution, which is to have a security consultant involved from the initiation of the project and review/rectify at an early stage to ensure that there is no separate lead time for security checks. The non-IT team should be able to ask questions to satisfy the risk conditions or take the escalation route. This is also an opportunity for organizations operating in silos to see and align business strategy and security, which creates a more lean, agile environment and ensures that hygiene is sustained.

**Technology**

Technology refers to software and hardware. It is important to understand how to ensure that installed software is the correct version and legally sound (i.e., obtained through proper purchasing processes) and to know how secure an organization's systems are (i.e., having the proper amount of security tools, ensuring that the servers are onboarded with proper configuration and versions, properly renewing security certificates).

Patches and upgrades are extremely important steps that are often not paid due attention.

For example, in a well-known data breach, the issue was that the organization did not complete patching on time. The need for patching and what to patch was identified, and recommendations were provided to the required teams. However, the final actions of initiating and completing the patches and audit verification did not happen. Vulnerability scans, which are supposed to uncover these issues, failed to do so. The process of monitoring and ensuring patching completion did not work as intended. These errors are due to a lack of discipline.

**Processes**

Every security policy should have required processes that align with respective timelines. For example, a policy around change management would say: “Each of the changes has to be adequately tested and test results verified and signed-off on before releasing to production.” This could well be ensured by documenting change management processes and following those processes in a disciplined manner.
Disaster Recovery
Another example of process documentation in alignment with security policy would be availability. Technology disaster recovery processes should be in place, reviewed to ensure up-to-date information, and tested adequately and frequently to ensure that the purpose is served. The purpose is the ability of the technology or application(s) to be recovered and return to normal operations (RTNO) within the agreed-upon time and based on the classification. Depending on the availability requirement from the organization, these applications should be architected and hosted accordingly, including recovery sites. Where an availability requirement is very high with no expected downtime, the required architecture should be different. It may even have mirroring solutions and, if there are any issues with the primary environment, the control will seamlessly be transferred to the secondary environment. Business or end users would not even be aware of a transfer. At end of the day, based on business needs and availability requirements, infrastructure must be provisioned. In short, the more the availability requirements, the more the cost involved in the setup.

There have been several IT outages, particularly in the airline industry, that have lasted more than one week, causing massive disruption to travel, inconvenience to passengers and financial loss. Because the impact of these events is critical, processes must be in place to bring the system/technology back to operational within a stipulated time. If the processes had been tested adequately and frequently, the systems would have returned to normal operations within a specified time. This is a discipline issue impacting security hygiene.

Business Continuity Outcomes Due to COVID-19
The COVID-19 pandemic has led many businesses to move toward nearly 100 percent remote work and connectivity. Until now, work from home for many enterprises was a dreaded concept because it increases opportunities for security risk for employees and stakeholders when they connect to the organization's network through their personal laptops or desktops. However, in many cases, there is no other option. In fact, the pandemic has led to people looking at new ways of operating organizations more effectively. For example, many organizations find that having employees work remotely cuts down facility and maintenance cost and are, therefore, shifting to this model for more and more employees.

Conclusion
IT security is everyone's responsibility, whether employees are part of an IT team or a business team. Strongly sticking to the basic hygiene in IT and IT security as identified by the organization is of foundational importance. Untrained employees are the weakest link in the chain. Employees across the organization should be trained periodically on key elements of security, such as how to keep up with security hygiene, either as part of onboarding or via refresher courses. Necessary audits should be conducted on a periodic basis to assess the knowledge level of employees and successful implementation of security practices. It is very important to have the right people in the right places who are willing to go above and beyond and are disciplined to ensure that security hygiene is developed and sustained in the workplace. Input from leadership is extremely important. It should resonate in each and every aspect of communication so employees throughout the organization understand and are able to deliver on the expectations of IT and IT security team hygiene practices to keep the organization secure.

Endnotes
1 International Organization for Standardization (ISO), 35.100 Open Systems Interconnection (OSI), https://www.iso.org/ics/35.100/x/
3 Corporate Finance Institute, “Enron Scandal,” https://corporatefinanceinstitute.com/resources/knowledge/other/enron-scandal/