# A Brief Guide to IT Hygiene

## What Is IT Hygiene?

Hygiene is a concept in the technology sphere that reinforces the idea of critical, regular, ongoing practices conducive to the health of your information technology (IT) infrastructure. While asset management is well understood within the IT and security space, IT hygiene is not yet a fully understood concept. With that in mind, it's best to start by defining what we mean by IT hygiene.

Adapting from Merriam-Webster, IT hygiene represents the conditions and practices that are conducive to IT health. In other words, IT hygiene is what you do, or should be doing, on an ongoing basis to ensure that your systems and services are safe, reliable, and available.

In the past, you could periodically review internal hardware and software assets to understand what belonged to your company. But digital transformation, and the accompanying speed at which infrastructures are changing, has made things more complex. Today, organizations must go beyond periodic management of hardware and software assets. These new complexities call them to continuously monitor and maintain digital and ephemeral assets as well. Organizations need an IT hygiene program in place to ensure business continuity and lay the foundation for other critical IT and security initiatives such as attack surface area reduction and cloud governance.

**Ultimately, an effective IT hygiene strategy encompasses your:**

- **Asset inventory:** What systems, devices, software, and services comprise your network.
- **People:** The individuals that make up your organization and their credentials and access.
- **Processes:** The structured work to manage components of the IT hygiene program.
- **Exposures and (mis)configurations:** The ways technology creates threat vectors that could be abused by bad actors.
- **Policies:** The agreed-upon ways processes must be mapped and carried out.

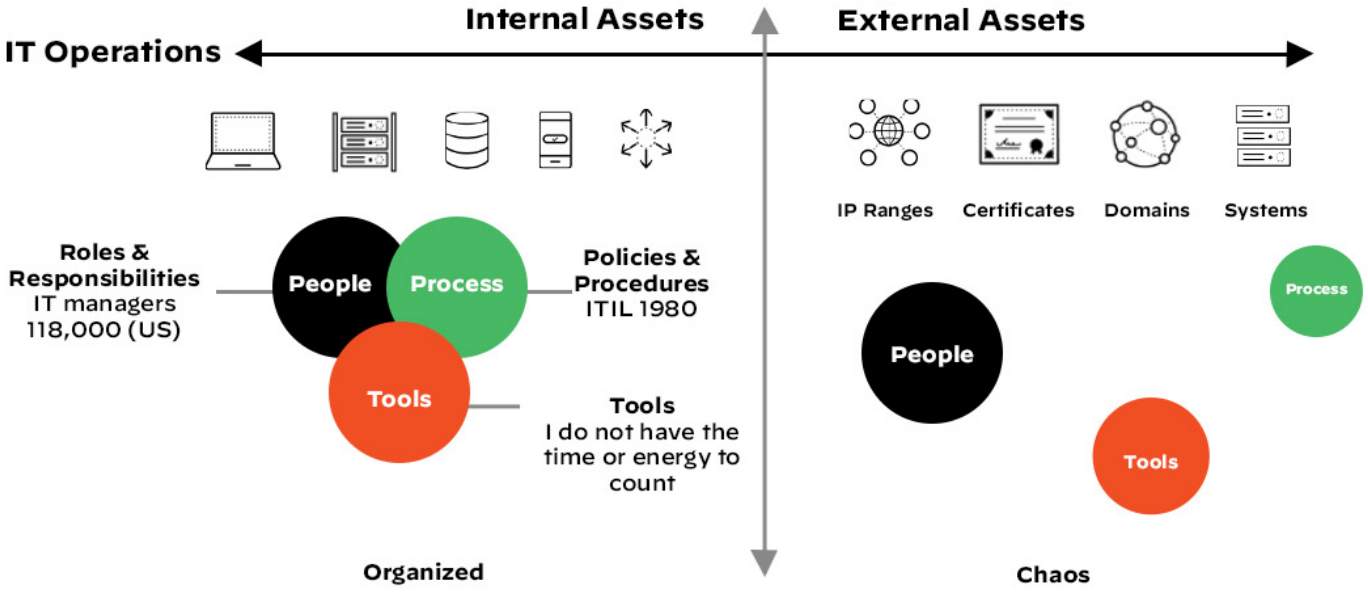


**Figure 1:** IT Operations

## Challenges to Effective IT Hygiene

The rise of cloud and democratization of IT makes IT hygiene increasingly challenging today. To reduce costs and boost agility, organizations have embraced cloud solutions, and 98% of organizations now plan to adopt multi-cloud architectures. At the same time, IT has also become more democratized, and anyone with an email address and a credit card can provision new infrastructure and short circuit established IT processes—the key pillar driving the rise of shadow IT.

Both of these trends only increase the pace of network change and make it more challenging for organizations to effectively manage their digital assets such as certificates, IP addresses, domains, etc. These assets do not fit the classic description of a "physical technology asset" and exist outside of traditional asset governance processes. But they are nonetheless business-critical and have a lifecycle just like hardware and software assets do.

While in the past, a periodic inventory of your assets may have been enough to know what you needed to manage and protect, this strategy no longer suffices. Because your network footprint is constantly in flux, it's impossible to maintain an accurate and complete inventory of all of your internet assets through manual processes.

Unknown internet assets can infiltrate your network in a wide range of ways, including:

- **Shadow cloud infrastructure as a service (IaaS)**
- **Internet of Things (IoT) devices**
- **Mergers, acquisitions, and divestitures**
- **Failures in manual processes**
- **Subsidiaries and franchises**
- **Supply chain organizations**

## The Danger of Shadow IT

Very simply, you can't control and protect what you don't know. If you don't have full visibility into all physical and digital assets belonging to your organization, you don't have an effective IT hygiene program in place to support the business.

For example, while you may have mandated only specific, authorized cloud providers be used by your company, your in-house developers may have built business-critical tools and applications on an unauthorized and possibly even unknown cloud provider. And because you're not aware of this, you may not know that there's a real business issue where the mandated cloud providers represent blocks to getting things done quickly and easily to keep your business running.

This is a scenario that's different from the classic "malicious insider" risk. This is a risk that comes about because of the distance between the strategic vision that drives IT hygiene and the tactical need to "get the work done." In today's world of cloud computing and services, a little knowledge is a dangerous thing. It's easy for both technical and non-technical employees to implement and effectively deploy "shadow IT" solutions. But lacking the training and know-how, they don't understand the risks they're introducing to the overall business by doing so.

Regardless of the cause, however, the risks are real. Data breach, data loss, cyberattack, and ransomware risks are significantly increased when unknown, unmanaged systems are introduced to your network. Because networks change frequently (even daily), the asset list you had yesterday is not likely to be accurate unless it's being continuously updated automatically. That means that if you're using a manual process for IT hygiene, such as self-reporting and an Excel spreadsheet, you're already behind.

## You Need a System of Record

How are organizations to solve this problem? A decentralized model by which assets can come on the network requires an automated process to discover, assess, and manage those assets. That's where having a system of record (SOR) comes in.

Cortex® Xpanse™ provides a SOR for all of your internet assets. You benefit from a continuous and accurate view of all devices, systems, and services on the internet. In addition, you receive real-time updates when significant changes happen, such as when infrastructure or configurations change, mergers occur, or new assets are put into production.

Having a SOR gives IT and security teams a shared view into the organization's internet assets; this makes it easy for tactical practitioners to stay on top of day-to-day changes and leaders to get easy top-down visibility.

You can automatically learn when a server or service is exposed. For example, when a database is accidentally exposed to the internet or a poorly configured remote endpoint is running Remote Desktop Protocol (RDP).

**With a single Internet SOR, you are empowered to:**

- Gain full visibility into all of your on-premise internet assets as well as infrastructure and assets across cloud providers.
- Continuously discover unknown assets and bring them under management.
- Develop processes and service-level agreements (SLAs) to drive the deviation between what is known and unknown to zero, and to ensure all assets are well-configured.
- Continuously monitor assets for indicators of compromise and unusual behavior to prioritize high-risk and high-impact problems (this helps to deliver the highest business value even with scarce resources).

As the pace of digital transformation and the adoption of multi-cloud architectures is likely only to increase, organizations can expect to continue encountering both strategic and tactical day-to-day challenges with IT hygiene. But with full visibility through the Xpanse SOR, it is possible to overcome those challenges and lay the foundation for IT and business success.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com


cortex-xpanse-A-Brief-Guide-to-IT-Hygiene-wp-050621