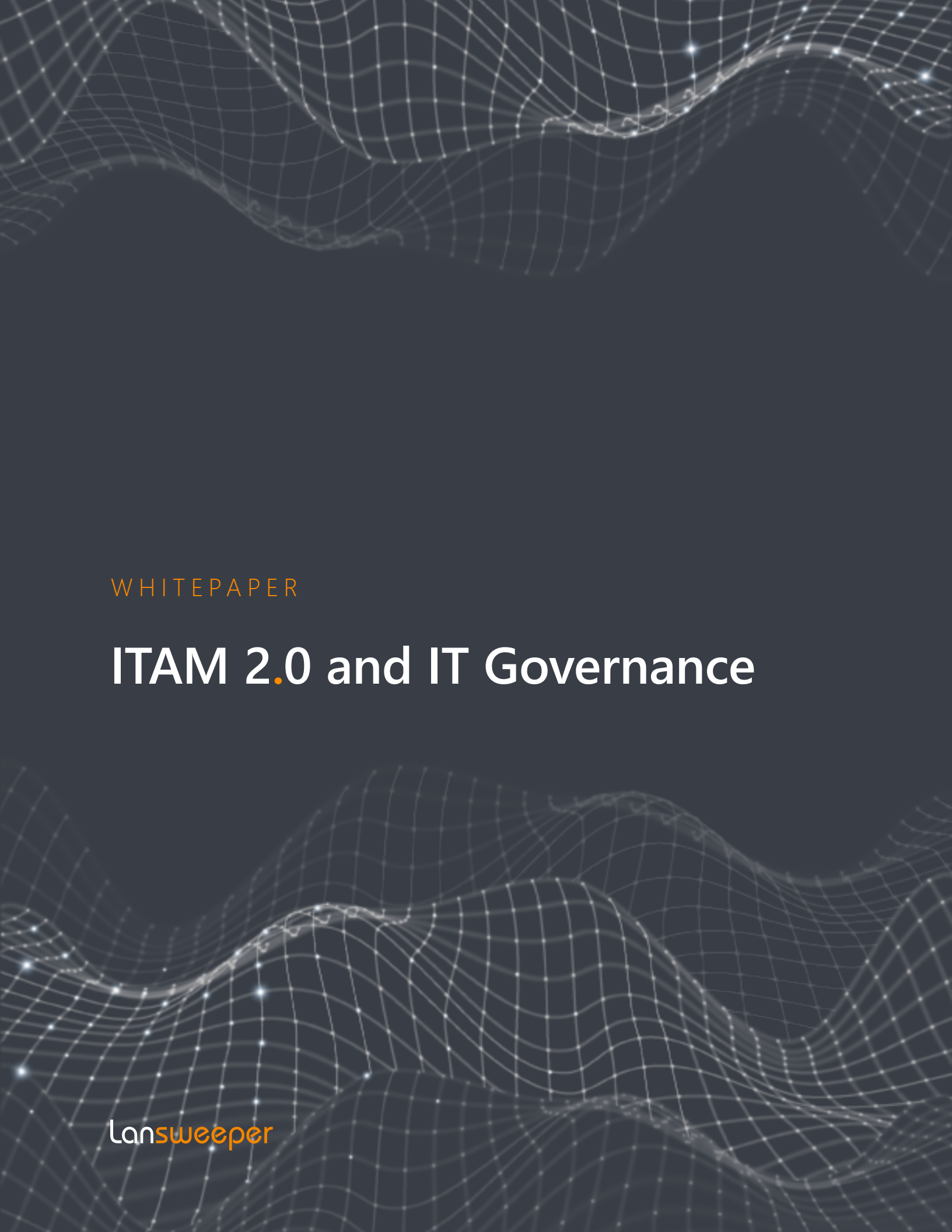


WHITEPAPER

ITAM 2.0 and IT Governance

Lansweeper

EXECUTIVE SUMMARY

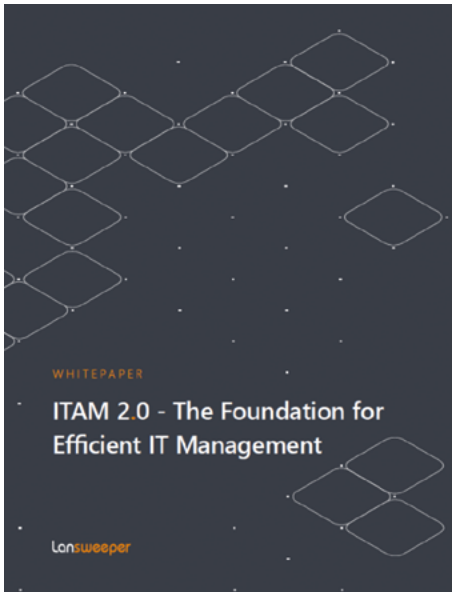
Solving the Visibility Problem

As the complexity and distributed nature of IT environments have increased, organizations have experienced a corresponding **decrease** in visibility into infrastructure, software and users. Because you can only manage what you can see, this dynamic is making it difficult to make strategic decisions across the enterprise, manage data silos, optimize IT spend and maximize data security.

As discussed in our white paper, "ITAM 2.0 - The Foundation for Efficient IT Management," the process for creating asset inventories must move beyond fragmented, scenario-specific collection of IT asset data. Modern IT governance – defined by Gartner as **the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals** – can only be achieved when centralized, comprehensive visibility has been established.

GET

The companion white paper:



ITAM 2.0 is designed to capture **all** the core objects of the modern IT infrastructure, software and users within an organization—not only hardware and software assets, but servers, mobile devices, virtual machines, containers and more.

In this whitepaper, we'll discuss:

- The critical need for accurate asset inventories
- Managing security threats—from inside and outside your organization
- The effect of IT/OT convergence on IT governance

CHAPTER 1

The First Step: Knowing Your IT

Lansweeper

CHAPTER 1

The First Step: Knowing Your IT

In the world of enterprise IT, governance is top of mind. Regulations set forth by governing organizations provide guidance to CIOs and CFOs on how to best track and manage digital assets within their organizations. In the wake of COVID-19 shelter-in-place orders, doing so is more critical—and complicated—than ever. Enterprises face increased security risks, as employees use home networks to access work data, files and applications, thereby introducing potential network vulnerabilities via connected home devices. That's why it's important to have an outstanding inventory management system.

30%

of all the hardware and software assets in a typical enterprise, about 30% are considered "ghost" assets—they're missing and can't be found.

Not only is IT governance essential to the security of an organization, it has a direct impact on other key priorities including profitability. Without proper IT asset management (ITAM), an organization's IT footprint grows uncontrollably leading to security challenges, cost inefficiencies and management challenges. Unused or outdated devices can add to operational overhead, wasting resources and inflating the cost of software licenses and services.

Nearly 66% of IT managers have an incomplete record of their IT assets. What's more, "shadow IT"—infrastructure and services implemented without formal approval from the organization's IT department, will increasingly be funded by business units, which means IT governance at the corporate level will be even more critical for tracking and monitoring assets on the network, to protect against security threats and vulnerabilities.

It's essential that companies have and are able to maintain a centralized, complete view of their IT assets; or they will become liabilities to an organization's security posture and ultimate financial success.

— Roel Decneut, CMO, Lansweeper

ITAM Is at the Core of IT Governance

Governance bodies that regulate enterprise IT strive to mitigate the risks and costs of neglected, outdated and vulnerable assets, and provide frameworks for defining how organizations implement, manage and monitor their IT infrastructure. Achieving certifications in these frameworks are milestones to organizational maturity. Many larger enterprises won't adopt technology from companies that do not have certain certifications, and failing to comply with data privacy mandates can result in hefty fines.

Some of the most important IT governance frameworks and regulations include:

- The Center for Internet Security (CIS) outlines 18 best practices dubbed CIS Controls™ that aim to address and prevent the most pervasive and dangerous enterprise security threats.

- ISO 27001 is an international standard that helps organizations manage IT asset security and provides a management framework for implementing an information security management system (ISMS) to ensure the privacy, integrity and availability of corporate data.

- The Information Technology Infrastructure Library (ITIL) is a set of detailed practices for governing IT service management (ITSM). This framework focuses on aligning IT services with the needs of business by defining processes, procedures, tasks and checklists that help organizations improve the value of their services rather than just provide IT capabilities.

- COBIT is a framework for helping businesses achieve key objectives for IT governance and asset management. COBIT 2019 offers guidelines for improving enterprise governance and management, particularly as more organizations are migrating mission-critical workloads to the cloud.

- NIST has a set of frameworks for various aspects of ITAM, including NIST SP 1800-5, NIST SP 800-53, and the NIST Cybersecurity Framework. All are designed to help organizations protect critical infrastructure.

- Data privacy mandates such as the EU's General Data Protection Regulation (GDPR) regulate how organizations collect and store individuals' personal data.

At the core of all of these frameworks is an essential activity—maintaining a complete and accurate hardware and software asset inventory. This best practice is listed as a top priority in CIS, COBIT, ITIL and ISO certification guidelines, because if you don't know what you have, you can't manage or protect it.

CFOs and CISOs Share Responsibility for ITAM

Given the cost and risk associated with subpar ITAM, CFOs are now intimately invested—and in most cases responsible for—enforcing IT governance. CFOs need to understand how many assets the organization owns, whether or not they're being used, how they're being used, and how to maximize vendor contracts. Having a single source of truth and an accurate record of all hardware and software assets, as well as details about how they're configured and who's using them—and whether or not they require updates or need to be retired—is essential to controlling IT spend and ensuring IT investments align with and support business objectives.

Lansweeper enables organizations to know their IT—see, understand and report on all of the hardware and software assets that exist on the corporate network. Lansweeper continuously scans the IT infrastructure and gathers information about all devices and all software on those devices, then creates a single, trustworthy, always up-to-date repository of that information, an asset inventory. A dashboard makes the information actionable, allowing teams to easily identify vulnerabilities and respond to security incidents. They can also create customized reports that can be used to identify where and when patches or updates are needed, or remove compromised devices from the network.

43%

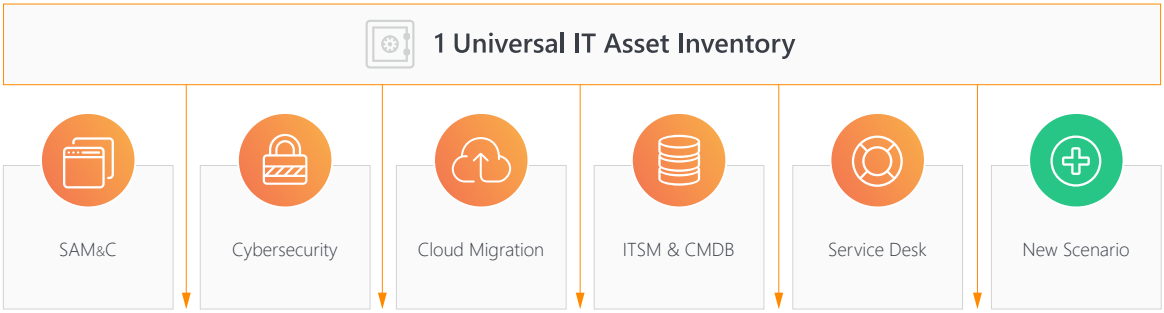
As a benchmark, a 5–7% decrease in operational costs will offset inflation and deliver measurable savings. This is where ITAM comes in.

Gartner:

Knowing your IT at all times enables you to save up to 30% of your IT budget.

> Lansweeper's technology bridges the gap between organizational silos, and between lines of business and corporate IT, to provide greater control and oversight for supporting—and complying with—IT Governance initiatives. Key here is the ability to detect what is truly there, not just what you know was purchased.
>
> — Roel Decneut, CMO, Lansweeper

In this way, Lansweeper's technology is particularly valuable for organizations looking to operate according to the leading IT governance frameworks. For instance, the second CIS control specifies maintaining a complete, accurate asset library. The COBIT 2019 IT Process Reference Model outlines five asset management essential practices: identify and record current assets, manage critical assets, manage the asset life cycle, optimize asset costs and manage licenses. And **asset management is essential for ISO certification**, which is often required to be a viable and credible technology vendor in the market.



The End Goal: A Productive Workforce

The year 2020 is upending business operations in many ways, and IT is at the center of the disruption. With more people working remotely and relying on cloud-based software services, cybersecurity, data privacy and IT spend will all continue to come under scrutiny. IT governance and ITAM is therefore an imperative, and organizations will be putting more effort toward this area moving forward. Leveraging technology like Lansweeper to create a complete IT asset inventory makes compliance with IT governance frameworks possible—and that reduces risk and spend.

CHAPTER 2

Stronger Security Through Better Visibility

Lansweeper

CHAPTER 2

Stronger Security Through Better Visibility

When organizations think about IT governance and security, they often focus on protecting internal assets and data from external threats. But what if the threat originates from within the organization?

According to Cybersecurity Insiders' 2020 Insider Threat Report, 70% of organizations say insider attacks are becoming more frequent. What's more, 68% report feeling moderately or extremely vulnerable to insider attacks, and 56% believe detecting insider attacks has become harder since migrating to the cloud. These statistics point to a growing possibility of exposure to threat from the inside-out by an employee, contractor or partner.

68%

of organizations report feeling moderately or extremely vulnerable to insider attacks.

Although organizations invest in security at the perimeter to ensure no outside threats infiltrate the network, they often neglect to safeguard the network from inside threats. Complete protection hinges on comprehensive asset discovery and management.

You're probably familiar with the "Trojan horse"—malware disguised as legitimate software. Hackers trick users via social engineering and other tactics, and load the malware onto a user's system to gain access.

When employees worked in the office, the bridge for the Trojan horse to cross was narrow and heavily guarded. Companies typically invest in multiple layers of firewall switches that can detect and prevent Trojan horses and other threats from getting in. Only the salespeople were on the road, and they would occasionally connect to the corporate network from their laptops over secure VPNs. But as more and more people take their devices outside the four physical walls of the organization, the devices become vulnerable and start posing a threat to the company network.

Why? When employees connect their corporate laptops to home networks, they open new gateways for malware, ransomware and viruses. They may use their work computers for personal endeavors, such web surfing, gaming or viewing entertainment, for example. An employee may unwittingly click on an add or download an app, and open the door for malware. This can happen easily if the user has local admin rights. You need the right tools to find all local admins in your network.

When employees connect their corporate laptops to home networks, they open new gateways for malware, ransomware and viruses.

Another major problem is that other devices that are not within the corporate IT department's purview are often connected to the home network, providing a conduit for hackers to connect to corporate devices. The Internet of Things (IoT) further complicates the situation, as in many modern homes, numerous IoT devices—think Alexa or Echo, smart heating systems and appliances, or video doorbells—are also connected to the home network. IT departments need to realize that the home network is becoming an important attack vector.

IoT devices have operating systems with software running on top, and although hackers usually have no interest in attacking someone's home network, they can leverage these devices, drawing on their processing power or using the devices as soldiers in the hacker's war to enter an organization. Malware can live undetected on a home computer or IoT device for days or weeks, building momentum before launching a large-scale attack, causing devastating damage and potential financial losses for the organization.

64 billion

By 2025, it is estimated that there will be more than to 64 billion IoT devices worldwide.

A Broader Approach to IT Governance

Until March of 2020, only 3.4% of the workforce in the U.S. worked from home on a regular basis. By April, about 20% of all U.S. employees were signing on from home, and for many organizations, 100% of their employees began working remotely overnight. Given this new, distributed IT environment, it's essential that organizations know and monitor what goes on behind the firewall, as well. What assets are connected to the network? Who's using them? How are they being used? Do they have the appropriate protections and up-to-date software installed? Are there vulnerabilities?

Until March of 2020, only 3.4% of the workforce in the U.S. worked from home on a regular basis. By April, about 20% of all U.S. employees were signing on from home, and for many organizations, 100% of their employees began working remotely overnight.

To answer these questions, organizations must progress beyond point solutions that address isolated aspects of IT governance, such as security. **IT governance in today's environments requires maintaining a single source of truth** that contains the depth and breadth of data necessary for all scenarios, including security outside and within the corporate perimeter.

ITAM 2.0: Everywhere Your Assets Are

Lansweeper enables organizations to rise to the challenge of ITAM 2.0, and protect their corporate networks using a bottom-up approach. With our IT Discovery & Inventory solution, organizations can collect, analyze and report on every IT asset within and outside of the four walls in real-time, at any time and for any use case, and gain unprecedented insight into the health and security of the entire infrastructure.

Having this information alerts IT to any potential vulnerabilities on unprotected networked devices that could pose a threat to corporate data and assets—a capability that's especially important now that the majority of the workforce is remote.

The basic premise of good cybersecurity is that you can't protect what you can't see. So the critical first step when it comes to basic cyber hygiene is to maintain visibility of your IT environments and develop the relevant daily routines to inspect and verify.

In terms of IT Governance, a single source of truth for all IT assets connected to the network is essential for compliance. Lansweeper reveals in easy-to-understand terms what devices have outdated antivirus software, OSes or other vulnerabilities that could open the door to malware or other threats.

> As opposed to scenario-specific tools that collect highly technical information on a subset of assets, Lansweeper reports can be tailored for different business audiences, providing detailed data and actionable insight to IT staff, so they can perform necessary updates and patches. Additionally it generates high-level reports tailored for CFOs and CEOs, to keep them informed at all times, without bogging them down with technical details.
>
> — Roel Decneut, CMO, Lansweeper

CHAPTER 3

IT/OT Convergence & ITAM 2.0

Lansweeper

CHAPTER 3

IT/OT Convergence & ITAM 2.0

Manufacturing has come a long way since the industrial age—digital transformation is accelerating as a way for manufacturers to reduce risk, optimize spend and control costs. As a result, operational technology (OT) and the IT assets that comprise it are proliferating at an unprecedented rate and the role of ITAM & IT governance needs to expand into OT.

Not long ago, OT was treated as separate from IT within the corporate four walls, and as a result, IT Governance best practices were not typically applied. That didn't matter so much in the past, because the systems were separate from corporate IT networks. Today, however, they're connected to corporate networks and systems, and organizations who neglect to extend ITAM to include OT will soon find themselves vulnerable to risk and increased costs.

Let's take a look at why organizations must extend IT governance to encompass OT and the myriad IoT devices connected to it, to ensure security and control operational costs as Industry 4.0 takes hold.

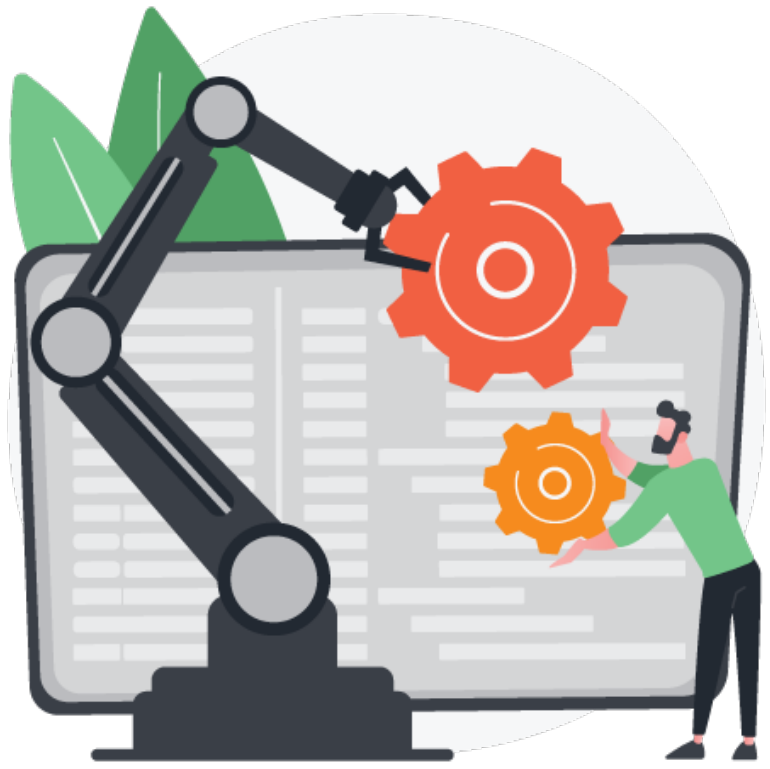
Industry 4.0:

A new industrial revolution that marries advanced manufacturing techniques with the Internet of Things to create manufacturing systems that are not only interconnected, but communicate, analyze, and use information to drive further intelligent action back in the physical world.

IT and OT Converge on the Network

OT consists of hardware and software used to monitor and control physical equipment, machinery, and processes in manufacturing environments. OT is found in industries that manage critical infrastructure—water, energy, oil and gas—as well as manufacturing facilities for automobiles, defense equipment, construction, pharmaceutical goods and so on. Through automation and integration with other business-critical systems, OT provides tremendous efficiencies.

Historically, OT was isolated from corporate IT networks. For example, in a printing facility, specialized software would instruct machinery when to dispense ink, and when and how to cut paper or other materials, but the PC running the software would interact only with the machinery it controlled. This was the typical OT scenario, and as such, securing the OT environment revolved primarily around physical security concerns. Since the devices were operated manually or with proprietary electronic controls, they didn't pose the same security risks as devices connected to the corporate IT network.



> The desire to cut costs and make operations more efficient led to the convergence of IT and OT. OT suppliers are now converging their systems onto connected IT platforms, to enable remote monitoring and management, reduce costs, improve vendor support, and streamline operations and management.
>
> — Roel Decneut
> CMO, Lansweeper

The Challenges of IT/OT Convergence

Converging OT with IT introduces new challenges—specifically, the potential to create vulnerabilities that expose the enterprise to security threats. One common trend we see is outdated software that is used to control industrial systems. A significant number of dedicated PCs in OT environments are running outdated Windows operating software, such as Windows XP, which is no longer supported by Microsoft and does not benefit from software patches and updates that could protect the network from new and emerging security threats. This presents easy targets for hackers, putting organizations at high risk of breaches and downtime. **That's why it's so important to have software like Lansweeper.** You need to properly identify and track these vulnerable devices so that potential risks can be identified and mitigated before they become a serious problem.

Another problem is that vendors are deploying software updates and patches remotely, in an effort to reduce the costs associated with sending support staff to facilities to update equipment. This means manufacturing facilities must open up their networks to outsiders on a more frequent basis. To make matters worse, OT environments have not been subject to the same IT Governance as IT, because they fall outside of the purview of those responsible for IT security, risk assessments and audits.

56%

of organizations that use industrial control systems as part of their OT experienced a security breach.

Research from a 2019 Forrester and Fortinet report found that 56% of organizations that use industrial control systems as part of their OT experienced a breach over the year prior to the study, and 97% said those breaches were a direct result of IT/OT convergence efforts. This is why securing OT is ranked among the most important digital transformation initiatives among cyber leaders for the next 12 months, according to Deloitte's 2019 Future of Cyber Survey.

IoT Adds Complexity, Extends the Attack Surface

Adding to the existing challenges of IT/OT convergence is the growing number of cloud-connected IoT devices. With increased automation, machine-to-machine (M2) communication and connected devices that define Industry 4.0 proliferating at a rapid pace, continuous monitoring of the entire IT estate is absolutely critical to minimizing risk and controlling operating costs.

IoT devices range from complex robots to environmental sensors to smart glasses and other internet-connected devices—and every device that's accessible over the corporate network can be the gateway for a malicious attack. Even "smart" coffee machines are a possible attack vector. Any vulnerability on these connected devices can put the organization at risk.

Picanol Group, a large manufacturer of weaving machines, fell victim to a large-scale ransomware attack in January of 2020, causing significant financial impact in downtime and costs associated with calling in experts to repair affected IT systems. When ransomware hit Norwegian aluminum giant Norsk Hydro in March 2019, the company's operations and IT systems were impacted, and its OT had to be switched into manual mode—a disruption that cost the company more than **$40 million**.

A Clear Path to Organization-wide IT Governance

A dedicated ITAM solution can become the foundation for IT governance and security across all of an organization's connected assets, and inform any possible use case—from cybersecurity to compliance, service desk, ITSM, cloud migration and more. At Lansweeper, we believe that our ITAM 2.0 solution makes this possible.

> Lansweeper's vision for ITAM 2.0 is to create a single source of truth for all data pertaining to any network-connected device—whether within the four walls of an enterprise, within manufacturing and production facilities or inside the homes of remote workers.
>
> — Roel Decneut, CMO of Lansweeper

Know Your IT!

You can't manage and protect what you don't know you have.
IT is most agile with a reliable asset inventory on-hand.

- Future proof approach to ITAM
- Agentless discovery
- Aggregating data across IT systems
- Cloud based for scalability and accessibility
- Leverage data for any IT scenario or use case
- Ability to integrate with other applications and services

For more information about Lansweeper, visit www.lansweeper.com.

Lansweeper