Guidehouse
outwit complexity

guidehouse.com

Asset Intelligence: Understanding Cyber Risk Across Your Physical, Technology, and Data Assets

Developing a comprehensive accounting of digital and related assets are a crucial first step toward cyber resilience in today's digital climate.

The relentless proliferation of technology in the workplace has contributed to the number of digital assets in the average organization multiplying drastically. Additionally, an influx of mobile devices and personal computers connecting to corporate networks is driven in part by remote work and the many personal devices that share home networks with work computers when employees work from home. This is challenging how organizations of all sizes manage cybersecurity.

These trends have created more complexity and greater risk across all areas of the organization as the network attack surface has continually expanded over the past few years. Organizations now have an unprecedented volume of endpoints, devices, unsecured Wi-Fi connections, and third-party tools accessing the network.

Each of these possible entry points—particularly the ones that are undetected or unaccounted for—has the potential to create new vulnerabilities and compromise the security of your organization.

With that in mind, asset intelligence should be a top priority in the current cybersecurity landscape, to ensure that everything attached to the network is logged and assessed correctly. Asset intelligence should be elevated to a critical issue, not just within IT, but also directly linked to the organization's overall mission and business strategy.

Put simply, if you are not aware of every asset attached to your network, it is not possible to fully secure and protect that network. This includes evaluating issues related to employee work-from-home environments as well. For example, if your employees are printing from home, are those prints being logged and tracked? If not, such knowledge gaps will put assets, day-to-day operations, and sensitive employee and customer data, as well as your business's reputation, at serious risk.

Organizations must assess and understand every single asset in terms of:

- Its physical health and maintenance.
- Its technological capabilities and interactions with the network.
- The data it uses, along with the sensitivity of that data, who has access to it, where it goes, and how it is used.

Fragmented Asset Management

Most organizations today are mired in a fragmented approach to asset intelligence and management. Network expansion has occurred at a pace that has been too difficult for asset management processes to keep up with or adjust to. As a result, there is rarely enough communication or visibility between departments regarding assets that are gaining access to the network, nor enough consideration for the implications that access has for cybersecurity.

True cyber resilience requires a strategic, collaborative approach throughout the entire business to ensure that asset intelligence processes are followed correctly. Rather than viewing this as an IT issue alone, education must be provided to demonstrate that meticulous asset management is a companywide responsibility. Only then will it be possible for gaps to be filled and all areas of the business to become more aligned.

Legacy Systems Lag Behind

As more innovative technology enters the workplace, assets that have been in place for a long time and are unique to your organization become more problematic. Many dated legacy systems do not have the technical capability to integrate with new software-based solutions, creating additional risk.

Significant work and development are necessary to ensure that asset intelligence is updated to encompass legacy systems, as well as to ensure that those assets themselves are secure in the context of your current estate.

Insufficient Asset Intelligence Creates Severe Risk

For organizations that lack asset intelligence and a companywide strategy for rectifying this problem, the following risks may become reality:

- The service and maintenance of physical assets will not take place if organizations are not aware of their status. This could result in lost data, unplanned outages, or failure of critical systems.
- Software vulnerabilities will go undetected, and the necessary patching will not be delivered, creating weak links in cybersecurity.
- Incorrect allocation of identity access management permissions will be more common, creating increased potential for leaking or misuse of data and other vulnerabilities.
- Cyberattacks or security incidents as a result of poor asset management place accountability and liability on the organization, especially if customer or partner data is compromised.
- Organizations face reputational risk if a cybersecurity attack or breach is made public and sensitive data is leaked or stolen and the organization does not have mechanisms in place to protect that asset or identify what data is compromised.

Why is the link between asset intelligence and cyber resilience underestimated?

The sheer speed of growth, the advancement of technology, and the digitalization of business operations and processes are too much to keep up with for many businesses. Organizations often dedicate so much energy to keeping pace with these changes that they can lose sight of some of the assets that might be putting the infrastructure at risk.

Comprehensive asset intelligence requires:

- A companywide shift in thinking, to establish strategic processes for logging, assessing, and securing all assets.
- Sophisticated tools for identity and access management over all end users.
- Proactive, rather than reactive, management and maintenance of the entire estate.
- Processes to ensure that failing legacy systems, obsolete assets, and replacement projects also feed information regarding any change into the appropriate places.

How to improve asset intelligence and increase resilience

There are many steps involved in building the level of asset intelligence that will enable an organization to become resilient enough to withstand today's sophisticated cyber threats.

- Conduct a thorough network evaluation to discover, log, and gain control of every asset—hardware and software—that is attached.
- Assess and classify assets, ensuring that all records are up-to-date.
- Implement processes to automate record and asset management.
- Bolster your security architecture to accommodate more structured asset intelligence (e.g., by segments, function, complexity, etc.).
- Manage how devices connect to critical infrastructure and use business roles to monitor access approvals for what devices or identities are approved to access the network.
- Introduce automated monitoring and reporting tools to identify changes or new vulnerabilities that might require patching or other security updates.

Minimize Risk to Become a Resilient Organization

Asset intelligence, when approached strategically, will significantly reduce cyber risk and minimize the potential downtime your organization will face in the event of any incidents.

Improving asset intelligence will also boost your business from a cyber resilience perspective, which is invaluable in the modern digital business landscape. However, it is important to understand that there is no quick fix or silver-bullet solution to overcome the challenges involved. Simply putting new digital tools in place and expecting them to handle this responsibility for you could be a costly error.

True resilience requires a combination of the right technology and processes, and an organization-wide culture shift to prioritize cyber risk management. These components allow you to form a wider strategy, aligning all departments to work together on the shared objective of fully securing your physical, technology, and data assets.

Contact

Amanda Kane
Partner, Cybersecurity
Akane@guidehouse.com

Jason Dury
Director, Cybersecurity
Jdury@guidehouse.com

About Guidehouse

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures, focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 55 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit **www.guidehouse.com**.

Web: guidehouse.com/cybersecurity / @GHTechSolutions / linkedin.com/company/guidehouse-technology-solutions/