Establishing Cybersecurity Intelligence

Identifying Risk and Vulnerability in IT Assets

VENTANA RESEARCH

Sponsored by B|DNA

A New Dynamic in Cybersecurity

Your organization is under attack, and that attack may be coming from unanticipated directions. The least recognized yet potentially greatest risk to your operation is a security breach of your IT assets. Every piece of hardware and version of software that is not maintained regularly could be a gateway for unauthorized access. What's needed is cybersecurity intelligence, a new discipline designed to protect IT assets from attacks.

Astute organizations realize the need to invest in cybersecurity intelligence. In our research on governance, risk and compliance, more than half (51%) of participants said that reducing their overall risk exposure is a priority – that concern was cited more often than any other.

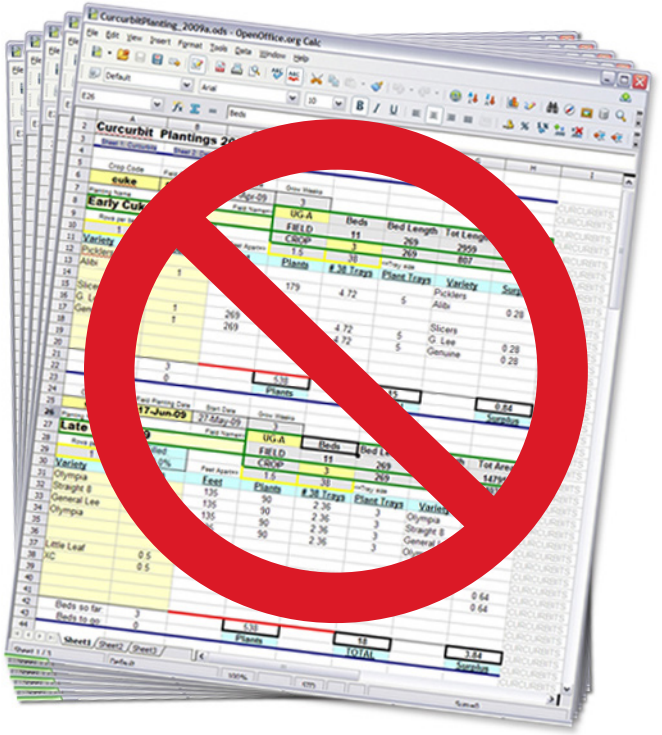
Takeaway: Embrace cybersecurity intelligence to secure IT assets.

Inventory IT Assets for Exposure

Large organizations have hundreds of different versions of software and complex arrays of hardware. To understand risk exposure **it's essential to continuously collect data about all technology.** Systems designed for this purpose can provide cybersecurity intelligence – knowledge that supports protecting the enterprise and its intellectual property.

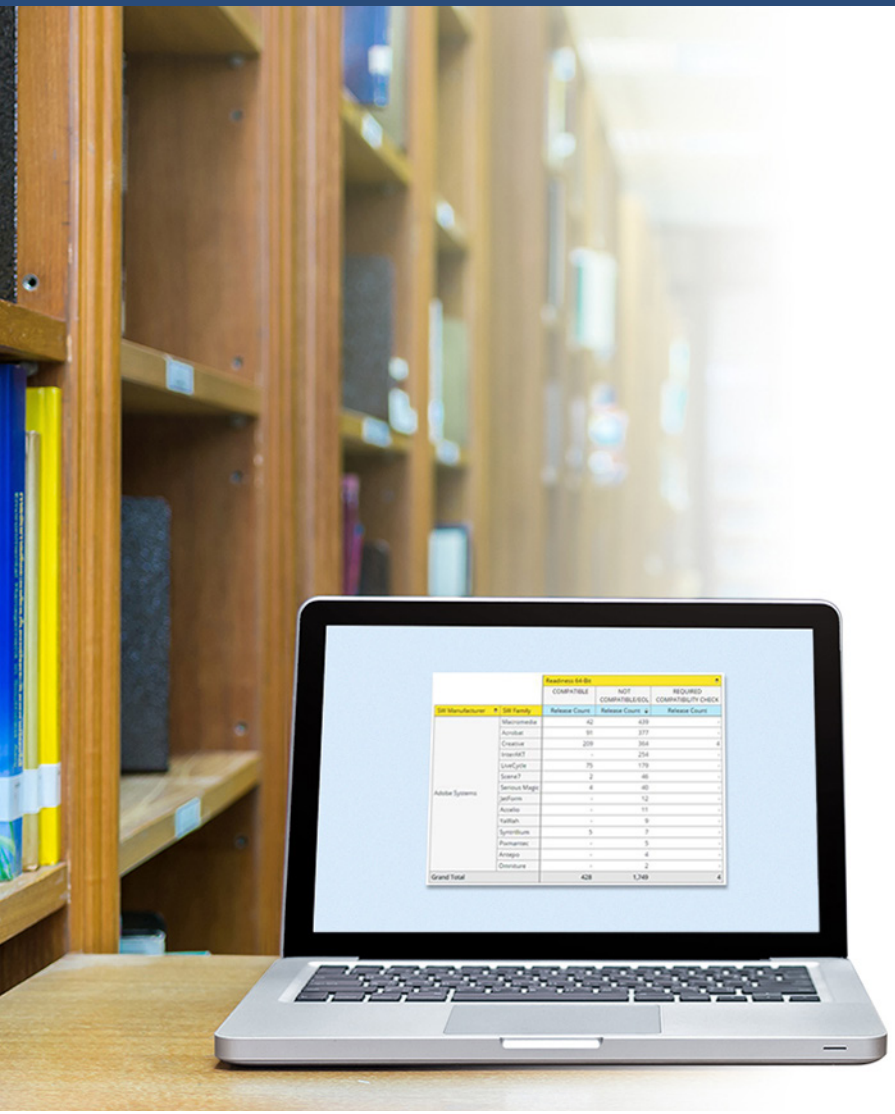
The first step is to inventory all systems by using IT asset management tools. This makes it possible to create an asset inventory. Continually reviewing the status of each item enables the organization to identify and close potential doorways to intrusion.

More than half **(54%)** of organizations said that preventing situations from occurring because of neglect is a benefit of such vigilance.



Takeaway: To minimize the risk of security breaches, inventory your IT assets for vulnerabilities.

Utilize a Catalog to Identify Risks



For a complete view of potential risks, **acquire a comprehensive catalog** from a third party that provides details on vendors, products, release dates and other details. Using one can reduce the time, resources and cost needed to manage IT assets. Match your technology asset inventory to it, and ensure your catalog is always up-to-date to support the analysis and actions that are required.

Compare your inventory and industry catalog with vendor-supplied version information to identify outdated technology and the greatest risks to the organization. Take action on immediate threats that could impact the security of IT assets and the information they contain.

Takeaway: Compare the IT asset inventory to an industry catalog to gain knowledge of risk exposure.

Use Analytics to Gain Visibility

To identify the most urgent vulnerabilities, summarize your inventory data by vendor, project and process. Then use analytics software with visualization capabilities to develop metrics to view aggregate-level risks and issues. **Analyzing IT assets can enable you to understand the impacts of retaining outdated systems.**

This sort of diligence is not common: Fewer than one-fourth **(24%)** of organizations said it is easy or very easy to access and use the data needed to measure and assess risk.

Takeaway: Use analytics to provide visual insight into issues and help prioritize potential cybersecurity threats.

Use Risk to Prioritize Changes

Manage your IT portfolio with up-to-date cybersecurity intelligence, using it to determine which technology projects require risk reduction most immediately. Understanding technology risk exposure by vendor and project will help you determine priorities for product acquisitions and negotiations with suppliers. Otherwise the organization is at risk unnecessarily.

Ensure that risk reduction is considered as a factor in replacing existing technology, especially when it is near the end of its useful life.

Takeaway: Make decisions about technology replacements or upgrades by assessing the risk profile of assets.

Use IT Asset Management for Cybersecurity

IT asset management is an essential part of cybersecurity processes, strategy and planning. It requires assessment and regular review of the technology inventory and issues related to it.

Additionally, **use internal incident and threat reports to sharpen insights** on threats from particular IT assets. The new ISO 27001 and 27002 framework offers guidance that enables management systems to bring risk under control through processes and reviews.

A dedicated approach for IT asset management is essential to reduce risk. Using spreadsheets to manage important processes such as inventory is haphazard and inefficient; more than half **(59%)** of research participants reported that using them creates problems.

Takeaway: IT asset management requires continuous inventory for effective cybersecurity intelligence.

Set IT Standards to Manage Risk

Use cybersecurity as an evaluation criterion by establishing risk and security standards for reviewing new technology. In particular, examine potential technology purchases, including supporting software and access points, for potential risks.

In organizations that must deal with many projects, systems and deployments, **applications dedicated to cybersecurity can enable IT to update governance policies** rapidly. Our research finds this is needed: Only 58 percent of organizations said they are satisfied that their approach is timely enough.

Takeaway: Do timely updates of processes and standards for technology use to prevent cybersecurity threats in the organization.

The Case for Cybersecurity Intelligence

An effective business case must demonstrate that addressing cybersecurity intelligence can reduce the risk of breaches and the associated cost of response. It also should **quantify the value to the organization of taking prompt action to avoid the most threatening cyber risks.**

Research participants **(79%)** most often said that identifying and managing risks faster is a means to take a more effective approach to governance, risk management and compliance.

It's also worth noting that using cybersecurity intelligence can help compliance with policies as well as with government edicts such as Executive Order 13636, which requires processes and concerted effort to address risks.

Takeaway: The business case for cybersecurity investments should emphasize the value of concerted efforts to prevent risks and exposure.

Act Now on Cybersecurity Intelligence

Addressing cybersecurity is essential to minimize risks that could threaten performance. We urge that organizations evaluate cyber vulnerabilities before an incident occurs.

Begin by establishing an ongoing process of assessing IT assets. Use a dedicated application to automate cybersecurity intelligence. Here again our research reveals a need: Only 37 percent of organizations said they are satisfied with their current technology to manage governance, risk and compliance. Comprehensively protecting your IT assets also can reduce the risk of damage to the organization's reputation.

Organizations that prioritize cybersecurity intelligence will be able to govern their IT assets and make new investments more wisely than others.

Sponsored by BDNA

The data in this ebook is drawn from *Governance, Risk and Compliance,* benchmark research by Ventana Research (**www.ventanaresearch.com**).

VENTANA RESEARCH