Developing a Strategy for IT Asset Management Success

By Allison Davis Ward, Partner

Have you ever looked at a chess board and thought about how confusing it all is? Which piece makes which move? How do you prevent your pieces from being captured? How should you deploy your pieces to win? The horse only moves in an L shape?! If you don't have adequate information before starting the game, it can be daunting to come up with a strategy for success.

Like learning chess, IT asset management can seem like a mountainous task, but strategic planning will make the task manageable and save you headaches and sleepless nights. Creating an inventory of all your organization's information technology and systems and a plan to manage them is vital. After all, you can't protect all your systems if you don't know exactly what needs to be protected.

> You can't protect all your systems if you don't know exactly what needs to be protected.

Setting Your Strategy

First, let's list some critical IT asset management tasks that likely occur within your IT department:

- Hardening and securing new systems before they enter production
- Making sure end-of-life systems and software are replaced in a timely manner
- Removing sensitive data from hard drives before disposal
- Ensuring systems have appropriate anti-malware protections
- Patching systems with firmware, operating system, and application updates
- Scanning IT assets for known vulnerabilities
- Ensuring critical data is included in backup and replication processes
- Confirming applications and software are properly secured with password parameters, account lockout settings, and multi-factor authentication
- Reviewing applications to ensure user access is restricted appropriately

The first step in playing chess is to understand each piece, and managing your IT assets is no different. What is the underlying need for the tasks noted above? You need to understand what "pieces" are to be managed within your organization by including them in the inventory.

While it's easy to start with items assigned a dollar amount, such as hardware and software, you should also inventory your data.

- Your **physical hardware inventory** should include hardware such as servers, workstations, laptops, mobile devices, firewalls, intrusion detection switches, routers, switches, printers, copiers, fax machines, and Internet of Things devices (e.g., Apple TVs, Amazon Echo, and other smart devices). Include critical details about each asset, such as location and warranty information.
- Your **software and application inventory** should similarly identify all software installed on systems and applications that employees access, including those with web-based logins. This inventory should include details such as the version in use, system administrator, web address, license period, and number of licenses. Follow these three steps to create your software and application inventory.
- Your **data inventory** should identify and classify the types of data stored. For example, public information that is available on your website is different from proprietary details about your organization or sensitive information about your constituents. Before

you can secure this data, you must inventory it to know what it is, where it is stored, and how it is accessed. With the advent of data protection regulations like GDPR and the Colorado Data Privacy Act, this data inventory can be particularly useful for seeing where potential data trails might be within your systems.

Planning Your Next Moves

Once you've developed these inventories, it will become easier to plan your next moves in the game of IT asset management.

The hardware inventory can help you:

- Plan asset retirement and determine when systems are reaching end-of-life and should be replaced
- See when a device with a hard drive is about to be removed from a production environment so you can take the necessary steps to ensure data is sufficiently removed
- Periodically reconcile to anti-malware and patch management consoles to help ensure that all systems are properly patched and protected
- Identify, for network equipment, which vendor websites you need to monitor for firmware updates and patches

The software and data inventories can help you identify:

- Which critical software or vendors you need to review periodically in areas such as financial stability, security controls, and business resilience
- Which systems and applications contain critical data that should have more stringent security controls
- Which systems you should evaluate regularly to ensure access rights are restricted
- When the licenses for certain products are ending
- What systems should be included in the backup schedule for immediate recovery and long-term retention purposes

These inventories can help your organization develop effective policies. For example, once you have full knowledge of what technology your organization uses, you can begin to develop policies and procedures governing the use of this technology and how it is implemented and secured within your environment. You can create acceptable use policies to ensure employees are aware of their responsibilities in using this technology. Finally, you can identify which technology needs recovery plans and procedures for business continuity and disaster recovery purposes.

Not too bad, right? The initial steps will always be the most difficult, but you can use the information outlined here to devise a plan to account for existing assets and develop procedures to ensure incoming assets are added to the inventory management system.

Once you have a strong process in place and get your IT assets in check, you'll quickly see how the rest of your IT management duties fall into place. You'll quickly master and win your game — checkmate!

> You can use the information outlined here to devise a plan to account for existing assets and develop procedures to ensure incoming assets are added to the inventory management system.

About the Author

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA