GUARDING LEGACY IT ASSETS

Cybersecurity For Unsupported Enterprise Devices

K7 SECURITY

Contents

Introduction

'Old is Gold' is a well known proverb, but it may not hold true in the world of computing and especially in the field of cybersecurity. Legacy devices present a cyber risk to businesses, a risk that is rapidly escalating in a world where cyberattacks are used to steal data, extort ransom, sabotage operations, and wage cyberwarfare.

Businesses are familiar with technology debt that is the result of systems developed in previous years, and how technology debt can increase challenges in integrating newer technology that could transform business operations. Businesses may not consider cybersecurity to be affected by technology debt, but the increase in cyberattacks across the world that result from the use of legacy systems necessitates a change in perspective.

This whitepaper will explore types of legacy systems, how they can impact businesses, and how businesses can protect themselves in an environment where the use of legacy IT is unavoidable and being targeted by cyberattackers is inevitable.

Why Legacy Devices Increase Enterprise Cyber Risk

All hardware and software have vulnerabilities and their vendors periodically release security updates to patch these vulnerabilities during a defined support period. No updates will be released by the vendor once the support period ends, but vulnerabilities will continue to be discovered. Enterprise risk increases along with the increase in the number of known but unpatched vulnerabilities in devices that the enterprise continues to use.

Software or hardware that is no longer supported by the vendor is described as having reached end-of-support. Such products will not cease to function when end-of-support is reached; they may continue to serve the purpose for which they are acquired, but increase the risk of a successful cyberattack against the organisation.

Cyberattacks That Have Been Linked To Legacy Devices

Enterprise cyber risk from the use of legacy devices is not theoretical or hypothetical risk estimation. Several real-world cyberattacks have been linked to the prevalence of legacy devices in the enterprise.

- **Water Treatment Plant in Florida** – Devices running on Windows 7 (which is no longer supported by Microsoft) coupled with other laxity in cyber hygiene allowed a threat actor to gain access to the plant's SCADA controls in an attempt to poison the water supply by increasing the amount of sodium hydroxide used to treat water
- **American Defence Contractor** – Devices running Windows XP (which is no longer supported by Microsoft) coupled with a lack of domain segmentation helped a ransomware attack to spread rapidly through the company

It is clear that legacy devices not only have a negative impact on cybersecurity, the impact is sufficient to threaten critical infrastructure and national security.

What Is Legacy IT?

The classification of legacy IT can vary by organisation, as technology that one organisation would never consider (e.g., mainframe systems) may be considered necessary for daily operations in another. Similarly, some organisations may have contracted with the vendor to provide extended support beyond the stated end-of-support date and therefore will not consider an IT asset to be a legacy resource; other organisations, however, will need to classify the asset as a legacy resource as they will not receive updates from the vendor.

IT teams can use the following guidelines to check if their organisation's IT assets should be classified as legacy systems or not in the context of cybersecurity. Any resource is a legacy resource if it

- Is not expected to receive security updates from the vendor
- Cannot be updated because of a lack of qualified personnel
- Cannot be updated due to its location or other physical constraints
- Cannot be updated due to financial constraints
- Cannot be updated due to the impact of downtime on downstream resources
- Is critically dependent on a legacy system from which cyberthreats may spread

The last point is often overlooked when evaluating the size of legacy IT in an organisation. Newer systems that are designed to be compatible and interface with older systems may be compromised through the older system; such newer systems should be classified as legacy even if they are currently supported by the vendor, if they are connected to a resource that cannot be updated.

Some legacy systems may have been developed in-house or are bespoke solutions and therefore identification of a vendor is not possible. In such cases, the classification as legacy (or not) should be based on the organisation's appetite to test the system for vulnerabilities and develop security updates to address identified risk.

Legacy IT systems need not currently be in use; they could be backup or redundant devices that are in storage or standby, to be deployed only if primary systems fail. They could also be partially in use i.e., four out of five functions of a device may be handled by newer systems, but the device may still be in use for one function alone e.g., a server may currently be in use only for authenticating building access but may have previously run several other applications as well.

Why Businesses Have Legacy IT

Why do many businesses retain legacy IT systems if they represent a cybersecurity concern?

Managing multiple business priorities with finite resources forces a choice, and the cost-benefit analysis of modernising legacy IT may not be perceived as favourable (especially in the short term) compared to investment in other areas. An upgrade may be desired but not feasible.

Let us examine a few reasons why organisations tend to retain legacy IT:

- If It Ain't Broke, Don't Fix It – The support period may have ended but the solution still serves its purpose. A newer solution may take a long time to integrate into complex business processes and the transition may be marked by long spells of disruption. Continuing with the legacy system appears to be the sensible option (provided a cyberattack does not occur)
- Continuous/Planned Obsolescence – Newer, more advanced versions of the IT solution will be continuously developed and released, leading to a perpetual replacement cycle. Organisations may prefer to retain the existing solution as long as it is functional, as waiting to upgrade provides an opportunity to acquire an even more sophisticated solution
- Partial Obsolescence – Industrial and healthcare equipment are built to be used for decades but the computing devices used to control them may become obsolete in a few years. In such cases, management may prefer to continue with the legacy controlling device than risk incompatibility between the newer device and the older software used to control the equipment
- Legacy Dependencies – The organisation may rely on custom-built legacy software that may not run on modern operating systems and the cost of rewriting the legacy software may be considered too high, resulting in the legacy operating system continuing to be used by the organisation
- Talent Deficit – The team or individual that created or deployed the original solution may no longer be available and the organisation may wish to wait until equivalent talent is recruited before attempting an upgrade
- Wide Prevalence of Legacy Systems – Organisations that operate in environments where legacy systems are the norm (e.g., 53.5% of Windows users in Armenia still use Windows XP) may not feel the need to upgrade their legacy IT because no one else appears to be investing in such upgrades
- Lack of Awareness – Organisations may be using legacy IT systems because they are unaware that some of the devices they use are now obsolete. This is more likely to occur in larger organisations that have a large number of devices, but can also occur in smaller organisations that do not have the resources to track device status

Why Businesses Underestimate the Risk from Legacy IT

Underestimating the risk from legacy IT results in underestimating the benefits derived from modernising or enhancing security for legacy IT, skewing cost-benefit analyses and reducing investment in such initiatives. There are several reasons that lead to businesses underestimating the risk from legacy IT:

- **No Attack Has Happened Yet** – This is an extension of the 'If It Ain't Broke, Don't Fix It' approach to IT. This may lead to underestimation of risk because
  - The attack may not have been detected – Threat actors can compromise a system and wait patiently for the right moment to strike. Additionally, not all cyberattacks aim to cause disruption. Some attacks are designed to exfiltrate data, either for espionage or for sale on the dark web; such attacks may not be detected for years
  - A new vulnerability could be discovered any day – AV-TEST registers 450,000 new cyberthreats every day. Any of those threats could be the one that wreaks havoc on a business through a legacy device. Threat actors seeking vulnerabilities in current systems may find vulnerabilities that also affect legacy systems e.g. the WannaCry ransomware exploited a software flaw called EternalBlue that affected older, unsupported Windows versions including Windows XP
  - System exposure may have changed – A device or application that was previously restricted to internal networks may now be exposed to external networks due to configuration changes in a different part of the organisation's IT ecosystem, significantly increasing the legacy system's risk
- **Backwards compatibility may introduce new risks** – A modern system may be designed to maintain backwards compatibility with older infrastructure, including support for insecure protocols and the deployment of software emulators. Such backward compatibility measures could result in the creation of new cyberthreats and also make the modern system vulnerable to threats that previously only affected the legacy system
- **Upcoming legislation may result in penalties** – Digital privacy and data security have become a priority across the world and many countries have introduced, and will introduce, legislation such as GDPR and HIPAA to protect personal information. Legacy devices may suffer from vulnerabilities that lead to violation of the provisions of these laws and result in severe penalties. Even if a legacy device may not lead to penalties under current laws, it could lead to regulatory action under future legislation, such as India's proposed Personal Data Protection Act

In addition to the above direct risks, indirect risks such as degradation of productivity can also result as the organisation will be limited by the capabilities of the legacy system even if other, more modern systems are deployed in the business. The legacy system will, over a period of time, emerge as a bottleneck that hinders operations across the entire organisation.

Industries that are At Risk Due To Legacy Devices

The manufacturing and healthcare sectors are conventionally perceived to be at risk of cyberattacks due to legacy IT, as industrial control equipment and medical devices are known to last much longer than the support window of their IT systems. 56% of healthcare providers rely on Windows 7.

This does not mean that other sectors do not rely on legacy systems. A survey by the US government showed that $60 billion out of a technology budget of $78 billion was spent on legacy investments, while a survey on the banking sector revealed that maintaining legacy systems consumes three-quarters of IT budgets. Many ATMs still rely on Windows XP.

Legacy IT has a pervasive presence in the business world and any business, large or small, in any sector is at risk if even a single unsupported device form parts of their IT infrastructure.

Protecting Legacy IT in the Enterprise

K7 Security recommends upgrading legacy IT whenever possible, as soon as possible. Currently supported IT solutions will always provide superior security when compared with unsupported solutions. However, we have discussed numerous instances where such an upgrade is not practical; we will now discuss mitigating measures that an organisation can pursue to avoid cyberattacks in situations where using legacy IT is unavoidable. These measures can be developed based on this framework:

Identify	Anticipate	Secure	Educate
Audit the IT Ecosystem	Create a Disaster Recovery Plan	Deploy Endpoint Security	Train Users
Analyse and Act On Audit Findings		Deploy Network Security	

Audit the IT Ecosystem

Understanding the depth and scale of a problem is essential to performing risk assessment and cost-benefit analyses. Every organisation must audit their IT ecosystem to generate a list of all legacy IT solutions that are present and identify their status. The audit must include:

- List of all computing devices, including networking devices (routers, etc.) networked devices (printers, IoT devices, etc.), NAS, and any other devices that are allowed to connect to the enterprise network including equipment that is leased, devices that are being serviced, equipment belonging to contractors, and personal devices of employees
- The operating system in use on the device should be noted, along with the update status of the operating system. Devices that rely on firmware may receive firmware updates which should be similarly noted. It is important to remember that a currently supported device becomes a legacy device if an update is available but has not been installed
- Patch status of all the listed devices, along with the latest available patch, should be noted. Similar to operating system updates, leaving available patches uninstalled turns a currently supported device into a legacy device
- Support status of the device should be noted. Vendors may or may not provide timely support to their products, and their support track record should be ascertained. End of support date for all devices should be noted
- The robustness of the credentials required to access these devices should be ascertained, as legacy devices are likely to be older and developed at a time when stringent access requirements were not enforced. The audit should particularly check if default credentials are in use. The audit should also check which employees are allowed to access the device, with an emphasis on identifying valid but unused credentials (employees who no longer use the device, employees who have left the organisation, etc.)
- All applications installed on the device should be listed, along with their support, update, and patch status
- The utilisation status (active use, occasional use, available for use but not in use) of the device should be noted
- Any data gathering or transmitting peripherals (photo scanners, barcode scanners, etc.) that are attached to the computing device should be treated and audited as separate devices
- Data that is stored on the device should be evaluated for sensitivity e.g., does the device store or route PII, R&D, or other confidential information
- Encryption standards on the device (types of data encryption, encryption at rest, encryption in transit) should be noted along with known vulnerabilities
- Protocols used by the device (communication, authentication, etc.) should be noted along with known vulnerabilities

Analyse and Act On Audit Findings

Once the audit is completed, the organisation should prioritise acting on the vulnerabilities that are discovered in the audit. It may not be possible to resolve all noted issues, but whatever can be fixed must be fixed immediately.

- Revoke access to devices and device access to networks if such access is no longer required, and initiate a process to ensure that access is always revoked as soon as the access is no longer required (such as when an employee leaves the organisation). This will prevent threat actors from attacking the organisation by taking over unused accounts. Other steps to prevent access abuse include:
  - Strengthen access credentials by changing default credentials and maintaining password hygiene
  - Ensure that each system has separate admin and user accounts, and user accounts do not have admin privileges
  - Implement Multi-factor Authentication (MFA) where possible
  - Prevent physical access to legacy devices to prevent device theft or data theft through direct access
  - Grant access based on the principle of least privilege i.e., a user has the minimum access privileges required to carry out their responsibilities
- Install all available updates and patches immediately for devices, operating systems, and applications. Initiate a process to track the release of updates and patches and their installation status. Investigate and resolve immediately if any update or patch fails to install
- Verify if devices that have reached end of support need to be used. If yes, disconnect from the network if network access is not required for current use
- Remove network access for all devices that are not currently in active use. Access should be granted only as and when required, and only for the duration required. If temporary access needs to be granted for a device that has reached end of support, implement a process to first check if a currently supported device can be used for the same purpose before granting access to an unsupported device
- Uninstall all applications on the device that are not in use, to prevent threat actors compromising the device through vulnerabilities in the unused applications
- Disconnect any peripherals that are not in use, and disable all unused ports
- Sensitive or confidential data that is stored on the legacy device should be transferred to another, currently supported, device. If storing such data on the legacy device cannot be avoided, ensure that it is protected through data access controls and encryption
- Configure the solution to use encryption or protocols that are secure and avoid the use of technologies that are no longer secure

Create a Disaster Recovery Plan

Create a disaster recovery plan specifically for legacy IT systems, keeping in mind that

- Obsolete hardware may be difficult to replace quickly, if at all
- Data backups that use the legacy system's proprietary data formats may still require the legacy system for data processing after data is restored from the backup

Deploy Endpoint Security

Endpoint Security is essential to protect computing devices, especially those that are no longer supported by the vendor. When deploying endpoint security, it is critical to ensure that

- All endpoints are protected by the endpoint security solution. Even a single unprotected device can open the doors to a devastating cyberattack
- The endpoint security solution must be allowed to receive all malware definition updates that are released by the vendor. With more than 450,000 new cyberthreats registered every day, endpoint security is only as good as its last update and endpoint security that is not allowed to update will immediately turn into a legacy system

When choosing endpoint security to protect legacy devices, pay special attention to

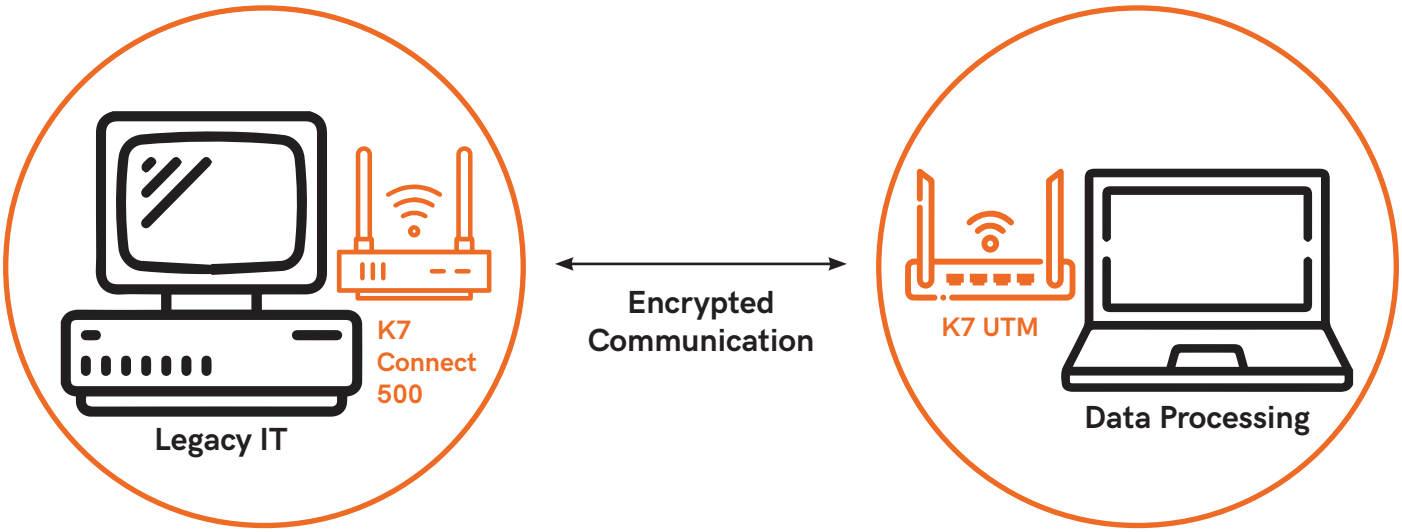
- **Efficiency** – Legacy devices typically run on older hardware that can be considered to offer modest performance by today's standards. The chosen endpoint security solution should not slow down the device. This is particularly important for mission-critical legacy computing devices
- **Legacy OS Protection** – The endpoint security solution should be capable of protecting devices running older, unsupported operating systems. The legacy protection should be provided out-of-the-box and not through a special support contract (which would indicate limited familiarity with legacy protection) and all protection and management features should be available on older platforms

K7 Endpoint Security is internationally recognised for its low-impact protection that does not affect device or network performance, and its OS support extends up to Windows XP.

Deploy Network Security

Not all legacy devices are endpoints or run on mainstream operating systems. Proprietary platforms and obsolete protocols make on-device protection a challenge. Such devices can be protected by deploying them within a protected network, creating a secure zone within which they can be used safely. K7 Security provides two network security devices that can protect legacy devices:

- **K7 Unified Threat Management (K7 UTM)** – The K7 UTM range of devices include Authentication, Authorisation, and Accounting (AAA) framework to control access to computing resources and a Stateful Packet Inspection (SPI) firewall to provide network-level attack protection
- **K7 Connect 500** – K7 Connect 500 provides encrypted VPN access in tandem with a K7 UTM device, enabling secure communication for legacy devices that lack encryption or include encryption that is no longer considered secure



Secure integration of legacy and modern IT systems using K7 Network Security solutions

Train Users

Once it is established that legacy IT systems are present in an organisation and represent a substantial risk, users of legacy IT systems must be trained to

- Avoid risk-enhancing behaviour, such as accessing internet resources from a legacy device or mention using legacy devices on social media (e.g., no reference should be made about using Windows XP devices at work)
- Notice and notify signs of threats or compromise, such as pop-ups requesting installation of software

IT teams will require additional training on risk mitigation, such as not allowing legacy devices to be used without deploying protective measures.

Planning for the Future

All IT systems that will be procured will turn into legacy systems someday. Businesses that wish to be proactive about cybersecurity should frame procurement guidelines to ensure that

- IT assets enjoy long-term support, and do not turn into legacy devices quickly
- The acquired IT assets will be easy to replace or secure when they turn into legacy systems eventually

Long-term Support

Long-term support should ideally extend through the useful life of the IT asset. We have previously discussed why this is not practical in the case of equipment that is designed to last for decades. In such cases, long-term support should extend well into the future i.e., the asset should not reach end-of-support within a few years of acquisition. Additionally, the vendor should commit to compatibility with the next generation of supporting systems e.g., Microsoft Windows 10 will reach end-of-support on October 14, 2025; therefore, the vendor of any software (including software used to control a device) should commit to Windows 11 compatibility to avoid the software only being compatible with an operating system that will stop receiving updates in a few years.

Given the timeframes involved, vendor's commitment to providing support and maintaining compatibility should be verified by checking the vendor's support track record.

Replacement & Legacy Security

Once any asset turns into a legacy system, as it inevitably will, it will be easier to replace with a modern system or secure with 3rd party solutions if it relies on open or industry standard protocols and formats. IT assets that rely on proprietary physical and digital interfaces present a much bigger challenge as legacy IT especially if they outlast the vendor.

Procurement of IT assets, therefore, should include evaluation of the solution's connectivity and data formats to ensure compatibility with solutions from other vendors.

K7 Enterprise Cybersecurity

K7 Security combines 30 years' expertise in cybersecurity with a state-of-the-art threat research lab to deliver multi-layered, rapidly updated enterprise cybersecurity solutions that protect critical data and devices in small and large organisations around the world.

K7 Endpoint Security

The international award-winning cybersecurity solution for desktops, laptops, and servers provides enterprise-grade protection against a wide variety cyberthreats including ransomware, Trojans, phishing, and zero-day attacks. Supported operating systems are:

- Microsoft Windows XP (SP2 or later)[32bit], Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11
- Windows Server 2003 (SP1 or later), Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019

All protection and management features are provided on older platforms, with no additional charges for legacy support.

K7 Network Security

K7's range of high-performance security devices provide gateway security and VPN solutions to protect your organisation's network and communications, and include:

- **K7 Unified Threat Management** – High performance gateway security hardware with AAA framework integration
- **K7 VPN Concentrator** – High performance VPN infrastructure for head offices, supporting hundreds of users
- **K7 Connect 500** – Cost-effective secure connectivity appliances for small branch offices, with built-in SIM support

K7 SECURITY

www.k7computing.com