An NCC Group Publication

End-of-life pragmatism

Prepared by:
Blake Markham, William Burlend & Robbie Joseph

Contents

1 Summary business context & target audience

With near daily reports of new attacks and data breaches, it is important that organisations take action now to avoid having their company name splashed all over the news. With forward thinking, and a proactive approach, technical security risks can be significantly reduced by implementing a sound IT Refresh Policy. One of the concerns associated with replacing IT infrastructure is the costs involved and the risk of introducing compatibility issues and, ultimately, downtime. However, exploitation of vulnerabilities in legacy systems and software can be damaging to an organisation on both a financial and reputational level.

This paper aims to identify and address these concerns and help with planning and replacing technology that is nearing or has reached its end-of-life (EoL) or end-of-support. This whitepaper should be useful for senior managers and stakeholders within organisations that are responsible for undertaking IT refresh projects, particularly when the focus is to minimise risk around EoL. The aim is to provide initial pragmatic advice on the various options available, how to go about planning a strategy for change and how to manage risk when EoL systems cannot be decommissioned, but must continue to operate.

2 What is end-of-life?

End-of-life is the stage in the product lifecycle where a product has reached a point where its vendor has decided that supporting the product is no longer profitable. This could be due to a new version release or an alternative product superseding its predecessor in the marketplace. Examples of software at this stage include Windows XP, Microsoft Windows Server 2003 and the Nokia Asha Platform. At the end-of-life stage, vendors will stop supporting and releasing new updates (including security patches), marketing and selling the product. The potential consequences for still-operational end-of-life systems are that any new, exploitable vulnerabilities identified in these systems will never be patched, rendering the underlying systems permanently vulnerable and exposed.

3 Protecting company assets

It is important for an organisation to identify what it considers as its most valuable assets and how it plans to protect them before any purchase of licenses or new hardware occurs. Examples of such assets include:

- E-commerce platform
- Personally Identifiable Information (PII) of customers and employees
    - Medical records
    - National Insurance numbers
    - Tax details
    - Addresses
- PCI Data
    - Credit card information
    - Financial records/statements

- Internal company documents
    - Contracts
    - Financial targets
    - Risk reports
    - Employee appraisals
- Company intellectual property
    - Designs
    - Source Code
    - Trade secrets

Listing what servers are important to the everyday running of the company, detailing exactly what software versions are running and the types of applications installed should all be documented and stored securely. Asset management software can drastically help an organisation when it comes to a technology refresh, saving both time and resources in determining infrastructure requiring replacement or maintenance, and constructing a timeline to support the refresh project.

Below is an example of a layout which can be used in budget meetings to demonstrate the business justification for such a project:

System	Description	Version installed *	Supported	RAG rating
Windows XP	Employee Desktop OS	SP2	No	Red
Apache Web Server	Customer Website	2.4.20	Yes	Green
MySQL Database	Product Database	5.5.39	Yes	Amber

* Information correct at time of writing

Assets can be identified from manual inspection tasks and/or automated scans across networks. While penetration testing activities are primarily aimed at identifying system vulnerabilities and documenting recommended mitigations for vulnerabilities that are found, they can also be used to derive network asset and version information.

Essentially, organisations should strive to implement and maintain good asset management. There are many different approaches and tools available to facilitate this depending on the organisation's technology makeup and network topologies. At a high-level, the following types of asset management tools might be leveraged by an organisation to home in on legacy and EoL products that are in operation on their networks:

- Software inventory tools - many solutions exist in this space which provide a level of automation in discovering devices and software in operation on networks.
- Licence management tools - where licensing is used within organisations for controlling and monitoring software use (particularly for commercial software), various licence management tools exist that can help maintain dynamic inventories of devices and software versions in use on those devices.
- Software deployment tools - organisations may use tools to automate deployment of new/updated software. Such tools typically provide a dashboard to show progress of deployment and thus can be used to track software versions on different devices.

- Patch management tools - such tools help automate deployment of software patches (security or otherwise) and also typically expose some form of dashboard to show patch compliance across networks.

A non-exhaustive list of platform-specific and platform-agnostic tools in this space can be found in section 9.1.

Note that many inventory/management solutions require installation of a software agent on each device that is to form part of an inventory/maintenance pool. Organisations should be aware of the potential risk with agent-based software. If a vulnerability in software agents is exposed, this might provide attackers with a mechanism of gaining unauthorised access to the underlying devices, regardless of the device's EoL status. Due diligence, security testing and patch management of agent-based software should therefore be performed to avoid the potential for weakening a network's security posture through agent use.

Once assets have been identified and risk assessed in terms of potential damage to the business, you will be in a better position to decide where you want to place them on your network and help allocate resources in an emergency. A lot of this type of information should be easy to obtain from the organisation's Disaster Recovery plan (IBM, 2015).

An IT refresh project can sometimes be a good opportunity to revise the company's network design with a more conscious security eye. Building a new network from the bottom up focusing on security will be invaluable if there is an attack on the company's infrastructure. It is difficult to create a one-size fits all network diagram as it depends on a range of different things such as how customers interact with the company, the type of data being stored and third party access. However, there are a few standard key points to take into account. Note that this is not an exhaustive list and there are many additional factors to consider when designing a network:

- DMZ between external parties and internal network
- Firewall
- Network segregation
- Intrusion Detection System (IDS)
- Web Application Firewall (WAF)
- Network logging
- Physical location
- Least privilege accounts
- Server hardening

The last element that requires protecting is the company's most important asset, its data. When new hardware has been installed, configured and data migration completed successfully, it is important to focus on securely disposing of the old equipment and hard disks. If these are collected by someone with malicious intent on exposing any residual data then it could prove damaging with costly regulatory fines and loss of business revenue due to reputational damage.

3.1 Legal & regulatory considerations

Not keeping technology up-to-date and secure will not only put your organisation at risk from malware and lack of technical support, but you may find you breach a number of regulations which could result in substantial fines. Some of the organisations with the power to impose fines are outlined below. However, it is important to understand that depending on your organisation, there may be other governing body rules that you need to abide by.

Data Protection Act (DPA) - 1998

Principle seven of the DPA stated, "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". This would include keeping user workstations and servers up-to-date with the latest patches and operating systems.

Fines of up to £500,000 can be levied against a company by the Information Commissioner's Office if an organisation is found to be in breach of the DPA. The DPA may eventually be superseded by the EU General Data Protection Regulation (GDPR), which, if introduced in the UK, will impose significantly greater penalties. In some cases, it can reach up to four per cent of the organisation's annual global turnover or €20 million (£18 million).

PCI-DSS - Payment Card Industry Data Security Standard – 2004

For non-compliance the corporation's bank could be fined between $5,000 and $100,000 per month. The banks will usually pass these fines back down to the organisation that breached the compliance rules. This may result in the bank terminating its contract with the organisation or increasing the transaction fees which could have a huge impact on small or independent businesses.

HIPAA - Health Insurance Portability and Accountability Act – 1996

A Community Mental Health Service was found to be in breach of HIPAA in 2014. This was because malware had found its way onto its network and compromised 2,743 individual's case files. This was due to a lack of basic computer security processes such as installing the latest vendor security patches. As a result, HIPAA imposed a $150,000 fine against the organisation and ensured future compliance by monitoring its security progress for the following two years (Office for Civil Rights, 2014).

4 Upgrade considerations

Being in a position to replace old hardware is a great opportunity to consider the market independently and the possibility of changing vendors. When putting contracts out to tender there are a couple of factors to take into account:

- How long the new technology should last (longevity/RoI)
- System interoperability
- Opportunity to merge applications together and remove redundant/legacy systems
- Move to a more virtualised estate (reduce running costs)

- Change vendors/analyse the market independently (don't be influenced by previous providers)
- If making legacy equipment redundant ensure it is securely disposed of (prevent loss of information)

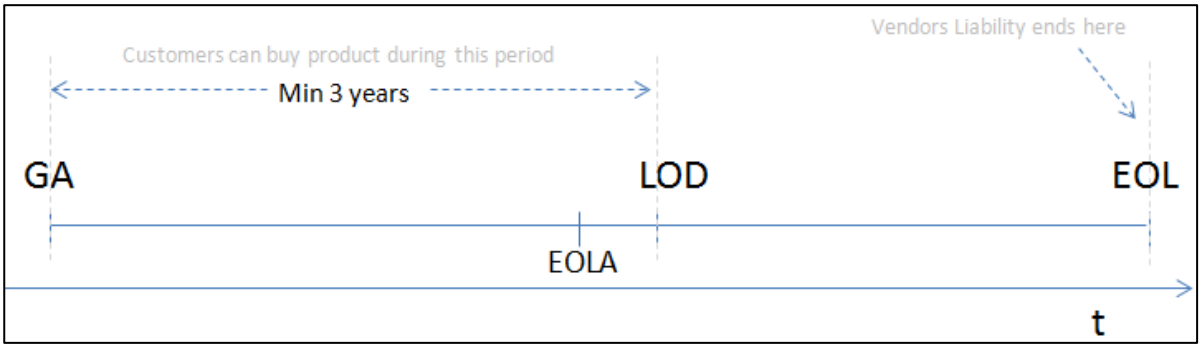

Figure 1 – Credit to Arkrishna (Arkrishna, 2016)

Figure 1 shows core milestones in a product's lifecycle. It begins with General Availability (GA) which moves to an End-of-Life-Announcement (EOLA) at some point dictated by the vendor. EOLA should then initiate a Last Order Date (LOD) after which point the affected product should no longer be purchased. From this point, up until the End-of-Life (EOL), organisations should be proactive in planning for managing EOL either through additional controls or product replacement/upgrade.

4.1 Updating estate benefits

Upgrading hardware and software during an IT refresh has numerous benefits to both the end-user and organisation. Not only does it provide Long Term Support (LTS) from the vendors ensuring security patches and assistance is readily available, but it will also help to reduce running costs as ostensibly modern technology is more efficient in both heat output and power consumption than older equipment.

When conducting an IT refresh, it is the ideal time to simplify the overall network and ensure fault tolerance and disaster recovery are built into the core design of the network. Over time, new servers and applications are installed and it can start to become difficult to maintain.

Recruiting a team to support a newer IT infrastructure will be easier to achieve and less expensive than a custom network with aging technology. This is because finding individuals with a very specific skillset means you might have to pay a premium for their knowledge and more time has to be invested to understand how the network is configured. In addition, it means that maintenance and support costs for an updated infrastructure should be more predictable which helps to allocate the correct amount of budget each year.

4.2 Embedded devices

Embedded devices are usually specialised computer chips that are used to perform specific tasks and processes. Embedded devices should also be incorporated into an EOL strategy. Organisations implementing an EOL strategy that has embedded devices, or will have embedded devices in the future through the use of Internet of Things (IoT), should take into consideration the difficulty of updating the firmware of IoT devices.

Dealing with hardware/embedded device EOL's is different from dealing with software EOL as mitigating software EOL can be as easy as just installing an updated version of software to a system, whereas updating an embedded device such as ICS and SCADA devices which are perhaps being

used for core industrial processes may pose more of a challenge as updating firmware that will be compatible with the hardware components of the devices can be difficult. Moreover, accessing the embedded device's physical chip in order to flash the updated firmware manually can also pose a significant challenge in some instances.

In order to update these sorts of devices, a technique called Firmware over The Air (FOTA) can be used. FOTA is a method of updating firmware on devices over the Internet which can be achieved by vendors developing their own firmware delivery infrastructures and pushing updates to end-client devices.

This method can also be implemented for use with non-Internet-facing embedded systems by implementing dedicated systems for retrieving firmware updates from vendors over the Internet and then pushing them internally to devices that need them, however, this can be financially costly and companies risk 'bricking' devices if there is a power outage, or if the update errors or is not completed properly for some reason.

The most common example of FOTA being used in the real-world comes from mobile vendors using this method to push updates to multiple devices simultaneously over the Internet.

4.3 Cloud & virtualisation

The continued adoption of cloud technology for platform and software as services (PaaS and SaaS) is likely to subtly change approaches to future software upgrade approaches and EoL management. Most cloud providers present an administrative portal for host deployment and management. As such, these portals will provide system administrators with a centralised mechanism for accessing, querying and inventorising product and software versions - this is in contrast to traditional networks whereby each individual device on the network might require discreet logins to access this information which can be time consuming on large networks and at risk of missing some devices during the process.

While cloud might not change the asset management approach for physical endpoint devices, it provides a centralised mechanism for managing and maintaining servers and any Software Defined Networking (SDN) or Network Function Virtualisation (NFV) components in use.

On the point of SDN and NFV, these technologies are quickly gaining adoption from the perspective of centrally managing entire networks or subnets within virtualised software environments. From an attacker's perspective, this means that if exploitable vulnerabilities exist in an SDN controller then attackers might be able to gain full control of an entire network through just one software exploit - managing EoL of future SDN/NFV solution will therefore be paramount to the security of organisations employing such technology.

However, it is important to note that the use of cloud will not necessarily provide a solution to EoL. While some cloud providers may provide options for automatic updates of specific operating systems or components, on the whole it will be the responsibility of an organisation to ensure that software within cloud environments is up-to-date, particularly if there are specific dependency requirements on bespoke software - it is unlikely that cloud providers would go too far in automating update of software for fear of breaking customer functionality, therefore cloud should not be seen as a solution to EoL, but rather a mechanism for helping to centralise the problem for improved management.

Organisations should review software update and EoL policies of their cloud providers in order to understand what (if any) assurances are given by the provider. Both Microsoft Azure (MSAZURE, n.d.) and Amazon AWS (AWS, n.d.) have policies in these areas.

4.4 When upgrading is not an option

Sometimes it may not be possible to upgrade a business critical system. Perhaps the cost of upgrading and migrating data to a new system is too large for an organisation to absorb, or the data is stored in a format that cannot be transferred to a newer system due to compatibility issues. If this is the case, then additional consideration needs to be taken to mitigate the associated security risks, taking into consideration that there is no risk-free way to continually use outdated software. The following section highlights a number of ways to reduce the business risks associated with products that have reached their end-of-life (ico., 2014):

- Ensure the unsupported software is not Internet-facing and is behind a firewall, IDS, IPS, or DMZ
- Ensure additional physical security controls are adopted such as CCTV, locked doors/ isolated storage or security guard
- Install logging software that records user access and actions taken on systems. This should be reviewed regularly
- Keep anti-virus software up-to-date
- Lock down unused ports/drives. For example, USB/CD/Firewire etc.
- Enforce a secure password policy
- Place adequate control around the device or product that has reached its end-of-life. This is essential to reduce the potential damage that a compromise could cause
- Where possible, isolate unsupported devices using air gaps
- Disable all services that are not needed (hardening)
- Remove wireless capabilities of legacy or outdated products if not being used
- Implement Full Disk Encryption (FDE) on hard drives (where possible)
- Set unique passwords, such that if there is a compromise the malicious party won't be able to get a deeper foothold on the network
- Prevent or minimise storage of sensitive data on EOL devices
- Prevent or minimise EOL devices form accessing any sensitive data
- Limit usage of the device
- Apply controls to the EOL device so programs/software from untrusted sources is not executed
- Move obsolete or outdated software to thin clients or virtual machines
- All Bring Your Own Devices (BYOD) should be treated as untrusted and unmanaged devices
- Segregate networks into specific VLANS

- All traffic to unsupported products should be monitored to prevent malicious packets
- An ops team should monitor for new 0-day releases and asses the likely impact on the organisation and its underlying technology
- Regular backups should be saved in case an issue is discovered with vulnerable unsupported software. This could be managed by virtualisation software taking system snapshots and securely storing them on a separate network

Implementing some or all of the above controls should place additional barriers for malicious users or attackers. However, as new threats are developed and released, the risks will always remain as no new updates or patches will be published by the vendor. The efforts above seek to reduce, not remove, the residual risk in maintaining operational EOL systems.

4.5 Risks of no EoL strategy

If your company does not have a suitable EoL strategy this could leave your systems exposed to a multitude of threats along with a non-compliant state.

The following areas are likely to be affected without a suitable EoL strategy:

- Lack of corporate direction
  - By not having an EoL strategy, an organisation may suffer from a lack of direction due to multiple different departments not adopting the same approach towards EoL devices. The lack of direction may also lead to uncertainty on the actions that need to be taken when a device reaches its EoL. Moreover, without an EoL strategy clear objectives cannot be set and responsibilities for achieving these objectives cannot be established.
- Ineffective use of corporate resources
  - Due to business plans and strategies being used to allocate corporate resources, it may be challenging to create and utilise resources such as finances and personnel without a coherent EoL strategy.
- Increased overhead from operational cost of unsupported systems
  - These systems will require ongoing extended support which will increase overall cost as well as further investment to keep the systems in a secure state.
- Failed IT audits resulting in a lack of compliance
  - Where a business (small or large) has annual audits to check if it adheres to set standards such as ISO-27001 and PCI-DSS with unsupported systems, the company will no longer be compliant. Not all businesses require compliance but for growing companies and those that handle credit card and/or other sensitive information this will be mandatory.

- Increased risk to the business
    - A business can expect to be subjected to greater risk from cyber security attacks as patches or bug fixes will no longer be applied to systems. This will ultimately leave systems open to a number of vulnerabilities.

This highlights the importance of preparing and implementing an effective EoL strategy to mitigate and reduce the overall risk and down-time to a business while the migration process is taking place. The main implications of lack of strategy include:

No updates:

- Current systems will no longer receive critical updates to protect.

No compliance:

- If industry standards are not met companies will cease to do business.

No safe haven:

- Cost will not decrease over time but instead will only increase without an EoL solution. What were once assets will become liabilities and increase overall operational costs.

It is essential to acknowledge the importance of end-of-life support regardless of what approach a business decides to take. It may be the case that current systems are running stable releases of Windows server or other variants of server software but this will not always be the case. As a result, the above will come into play leading to insecure infrastructure, increased overhead, non-compliance and insurance companies not willing to cover outdated systems.

There are multiple organisations that have either accepted or are unaware of the risks associated with unsupported software. Examples of such organisations have been reported in the press which has the potential to damage their reputation as well as highlight to malicious organisations and individuals that they could be vulnerable to common exploits. The Royal Navy has been criticised for using the unsupported Windows XP operating system on-board its Vanguard-class submarines which carry nuclear-powered ballistic missiles. Due to the operating system it runs and the type of work the submarines carry out, the risks of attack are increased substantially. The Ministry of Defence released a statement which said: “Submarines operate in isolation by design and this contributes to their cyber resilience” (The Guardian, 2016).

Another example of extending the use of obsolete operating systems can be seen with the US Navy. It has been reported that the US Navy has paid Microsoft to keep unsupported workstations operational and fully patched against new security vulnerabilities. The whole contract which is due to run into 2017 is estimated to be worth up to US$30.8 million. This is only a stop-gap while it executes the IT refresh project to remove unsupported operating systems from its estate (IT World, 2015).

5 Cyber liability insurance

Cyber liability insurance is an insurance product used to protect individuals and businesses financially in the event of a cyber data breach. This type of insurance product has been around for many years and typically tends to cover:

- Loss or damage of data as a result of the cyber breach
- Income lost due to downtime

- Reputational damage
- Ransom demands
- Expenses associated with notifying stakeholders of breach
- Cyber breach investigation costs
- Cyber breach remediation cost
- Costs associated with loss of intellectual property
- Costs associated with breaching regulation and contractual liability

These insurance products may provide a level of financial protection around EoL systems in the event of a breach experienced and attributed to exploitation of vulnerabilities in such systems. Note, however, that in the event of such a breach, while cyber liability insurance might help foot the bill of any associated legal or regulatory fines, the vulnerability in the underlying EoL system will still be present and thus at risk of future exploitation unless the affected system can be updated or further controlled from a security perspective. Additionally, such a breach would inevitably increase the insurance premium thus incurring cost.

It is also important to note that if cyber liability insurance is chosen as a financial protection against EoL, then organisations should ensure that the chosen insurance product policy suits the business needs. Some insurance providers and policies may explicitly state that compromise as a result of EoL vulnerability exploitation will not be covered, thus rendering the insurance product useless for systems comprising EoL products and software.

6 The IT refresh approach

Regardless of the size of the organisation, it will have to decide what is best suited based on the risk posed to their business regarding the systems reaching their end-of-life (EoL) and the variations in budget to replace those obsolete systems. In order to address potential risks that may arise from continuing an EoL product, a business will need to decide what action to take.

Here is a list of likely scenarios:

- Continue to use existing system which will become unsupported
- Target only business critical systems for upgrade
- Agree to purchase an extended customer support from the vendor
- Implement a dedicated security solution to monitor the unsupported systems
- Overhaul entire infrastructure with up-to-date systems

Utilising a roadmap of the hardware and software lifecycle will help in preparing an approach well in advanced before those systems reach their EoL. Incorporating a two or three-year plan prior to the expiration of the systems will ensure enough time to organise the most suited approach for the organisation. Conducting initial research into the organisation's current status in relation to its EoL strategy will help to identify where the process can be improved especially when an organisation is considering an EoL for the first time.

6.1 Small to medium enterprises

Small to Medium enterprises (SMEs) need to consider that budget constraints may impact on their end-of-life solution. This will vary depending on how heavily the organisation relies on its infrastructure and the information that is stored on those systems which will at some point require maintenance either through patching or an overhaul of systems due to the termination of support.

The decision on what will be the best approach will need to be considered in relation to these factors. The business will need to address any constraints either financially or through any approaches that may interfere with day-to-day business activities. This may include migrating old systems to the newly deployed systems without disrupting service. Identifying business critical systems would take priority looking at the current status of those systems and what information is being stored on them in relation to the associated business risk.

Once the most critical systems have been identified, it will be a matter of slip-streaming the transition from the obsolete to the newly deployed systems. Establishing a way point now allows for the business to decide the correct strategy of best fit to the organisation. SMEs may benefit from looking at any residual value remaining of their current systems which may be of use, and taking into consideration the lifecycle of its systems will benefit in the overall approach to an end-of-life strategy.

The final approach will consist of the following adopted strategy which will be tailored and altered based on the organisation in question but will provide a framework for the approach:

1. The organisation will adopt a systems lifecycle style of thinking to be able to prepare for system EoL two or three years before this end date is reached. This will initiate the EoL strategy.

2. Assets will be assessed to prioritise the deployment of replenishing the EoL systems. The remediation process will begin once high and low risk assets have been established providing structure and direction to the strategy when moving forward.

3. Implement a suitable solution to the business critical systems based on what has been prioritised and for what the budget allows.

Organisations that are of a larger stature may benefit from the increased revenue which can be used to improve their security. However, the approach would not necessarily differ as providing the most cost-effective solution will help keep within a set budget regardless of organisation size. This will be a matter of tailoring the EoL to the business and its requirements.

6.2 Migration strategy

Assessing business needs:

Using the above as a wireframe, the business needs to assess its needs and make a structured plan.

- Outdated servers to be upgraded.
- Custom builds to be accounted for to allow additional resource to migrate or upgrade.

Once the current situation has been evaluated consider the options based on this initial evaluation:

- Can current servers be virtualised or moved to the cloud instead of physically held onsite?

- Would ongoing support regarding updates be necessary based on the systems being upgraded?

- Is it worth introducing network segregation on certain servers?

Migration:

- Older applications will need to be assessed to address potential compatibility issues which could affect the migration process. Consider the best solution for the business. If new systems are required it may be suitable to look into a cloud solution. Transitions from 32-bit to 64-bit may not always be simple or cost effective.

- If there are custom builds within the infrastructure these may need to be configured and redesigned which may impact various elements such as file sizes and compatibility regarding various formats.

- Prior to any upgrade obsolete and no longer supported hardware such as network attached storage and switches need to be addressed as this could cause a costly delay during the migration and upgrading process. All of the above may be a large cost to incur initially but for a long term strategy will aid in reducing overall cost with the benefit of better performance and efficiency.

During the migration process it is important to engage with specialists to help with the overall migration and planning, particularly if this is the first time a large tech refresh or transformation has been performed by an organisation. The objective is to make things run smoothly and to reduce the amount of time to complete the migration. Once complete the outcome should result in virtualising where possible, and consolidating the amount of servers to maximise the investment. The UK Government has provided some guidance around managing obsolete platform security (GOVUK, n.d.)

7 A note on software escrow

Where organisations make use of bespoke software developed by third parties there is a risk to future maintenance and support of such software should the third party fail to maintain contractual agreements on maintenance and support, perhaps due to bankruptcy.

Software escrow services help assure the long-term availability of business critical software. This is where third party escrow agents maintain secure up-to-date repositories of such software to ensure maintenance of the software in the event of development halting by the third party. Escrow is somewhat-related to EoL since the demise of a third party software company inadvertently brings about an immediate EoL to the software it produced. Organisations should therefore consider use of escrow services for business critical software provided by third parties such that continued development can be performed (particularly if addressing security vulnerabilities in the code) and its lifespan extended (NCC, n.d.).

8 Conclusion

Developing an effective EoL strategy is key to ensuring the future security of a network's infrastructure and data. This paper has covered the main areas that need to be considered when deciding on the approach an organisation should use when thinking of or deploying an EoL strategy. This paper should be used only as a guide to help organisations plan their path to a better understanding of EoL and why it is important.

Simply monitoring and staying on top of your EoL devices is not a protection or mitigation. Awareness of EoL exposure is of course the important first step, but awareness of risk does not mitigate that risk.

While insurance products might provide some financial compensation in the event of a system compromise, using such insurance products purely due to known EoL systems in operation is not the best approach to reducing risk. If a company can demonstrate they have, or can implement sufficient controls to protect IT assets then this might of course help reduce insurance premiums while minimising the risk of compromise at the same time.

As part of cyber resilience and maturity, organisations should engage in routine security tests and audits to help understand their exposure whether through EoL systems or otherwise. An analogy here is with motor vehicles and the requirement for MOT testing – while a vehicle may be old and no longer manufactured, providing it can demonstrate roadworthiness and pass specific tests then the fact that it is no longer made/supported should not be a cause for concern. The same should apply to EoL – providing suitable controls are in place and that regulatory/compliance requirements can be met, organisations should be able to follow a risk-based approach and continue to run EoL systems, particularly if the associated costs of updating are unattainable.

Finally, all products will one day reach their end-of-life so having a strategy in place to help your organisation deal with these changes can, and will save your organisation time and money, as all parties involved in the upgrade process within your company will have a clear plan in place to achieve the overall organisation objectives.

9 References & Further Reading

Arkrishna. (2016, February 25). *End-of-life (product).* Retrieved from Wikipedia: https://commons.wikimedia.org/wiki/File:ProductEndOfLifeCycle.png

AWS. (n.d.). *https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf*.

Cabinet Office. (2015, November 30). *IT Health Check (ITHC): supporting guidance*. Retrieved from gov.uk: https://www.gov.uk/government/publications/it-health-check-ithc-supporting-guidance/it-health-check-ithc-supporting-guidance

GOVUK. (n.d.). *https://www.gov.uk/government/publications/obsolete-platforms-security-guidance/obsolete-platforms-security-guidance*.

IBM. (2015). *IBM Knowledge Center*. Retrieved from Example: Disaster recovery plan: https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_73/rzarm/rzarmdisastr.htm

ico. (2014, May). *Protecting personal data in online services.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf

IT World. (2015, June 22). *The US Navy's warfare systems command just paid millions to stay on Windows XP.* Retrieved from itworld.com: http://www.itworld.com/article/2939255/windows/the-us-navys-warfare-systems-command-just-paid-millions-to-stay-on-windows-xp.html?nsdr=true

Microsoft Windows Server 2003 End-of-Life. (2015, June). Retrieved from http://mytek.net/: http://mytek.net/windows-server-2003-end-of-life/

MSAZURE. (n.d.). *https://support.microsoft.com/en-us/help/18486/lifecycle-support-policy-faq-microsoft-azure*.

NCC. (n.d.). *https://www.nccgroup.trust/uk/our-services/software-escrow-and-verification/*.

Office for Civil Rights. (2014, December). *BULLETIN: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software.* Retrieved from U.S. Department of Health and Human Services: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/enforcement/examples/acmhs/acmhsbulletin.pdf

The Guardian. (2016, January 16). *'Trident is old technology': the brave new world of cyber warfare.*

Retrieved from The Guardian: https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare

9.1 Windows/Linux Software Asset/Version Management Tools

Windows Asset/Inventory Management Tools

- SCOM - https://technet.microsoft.com/en-us/library/hh205987(v=sc.12).aspx
- WSUS - https://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
- MS SAM - https://www.microsoft.com/en-us/sam/use-cases.aspx?CollectionId=9d33c0b2-7c54-4274-8b1c-d1dec3b8548d
- MAP - https://technet.microsoft.com/en-us/solutionaccelerators/ff807352.aspx
- MBSA - https://www.microsoft.com/en-gb/download/details.aspx?id=7558 (note Windows 2000 is no longer supported with this release)

Linux Asset/Inventory Management Tools

- Vuls - https://github.com/future-architect/vuls
- Spacewalk - http://spacewalk.redhat.com/
- The Foreman - https://theforeman.org/
- OS Query - https://osquery.io/

Multi-Platform Tools

- Solarwinds - http://www.solarwinds.com/
- BMC Atrium - http://www.bmcsoftware.uk/it-solutions/atrium-cmdb.html
- OCS Inventory - http://www.ocsinventory-ng.org/en/
- Chef - https://www.chef.io/chef/
- Snow https://www.snowsoftware.com/int/sam-solutions