Unsupported Software: The Hidden Weak Link That Can Harm Your Business

By David DiLeo, CTO, Epilogue Systems | 01.12.2023

Cybersecurity and compliance risks are ever changing
How does unsupported software impact your business?
What to do? Be proactive

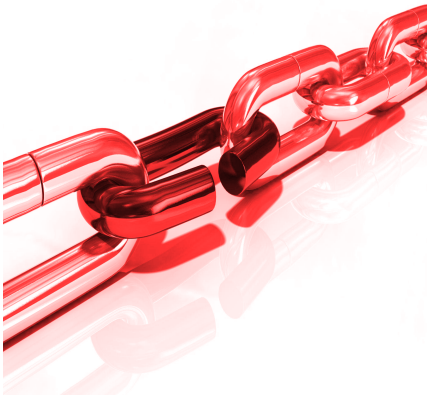
Unsupported Software: The Hidden Weak Link That Can Harm Your Business

Cybersecurity and compliance risks are ever changing

Ensuring that a company's physical and digital assets are effectively protected from external and internal threats is a top priority for any Chief Information Officer or technology leader. This is no small task when you consider the challenge of navigating an ever changing technology landscape, increased levels of attacks, and complex domestic and global compliance requirements.

To help combat this volatile and sometimes hostile reality, thankfully, cybersecurity has become mainstream. It receives plenty of media coverage and is now recognized by most companies as an essential and critical business function. It is also receiving increased federal and private funding year-over-year fueling a strong cybersecurity software and services sector that is growing exponentially. While this is all positive, it does not simplify the technology and compliance landscape. It also does not eliminate the bad actors – they still hack. Lastly, it does not reduce vulnerabilities – software will still have bugs. Every new piece of hardware and software that comes to market brings along a plethora of new risks and exploitation opportunities. As such, dealing with cybersecurity risk and maintaining compliance is a never-ending journey.

Some aspects of managing cybersecurity risk are quite obvious and the basics quickly come to mind. This might include hardening company infrastructure, implementing appropriate user access controls, ensuring all technology assets have anti-virus software, and educating employees to avoid email phishing attempts. Of course, there is much more to be done and companies do not have to figure all of this out on their own. Many mature cybersecurity frameworks are available to companies such as the NIST Cybersecurity Framework to help guide the creation of a robust cybersecurity practice.

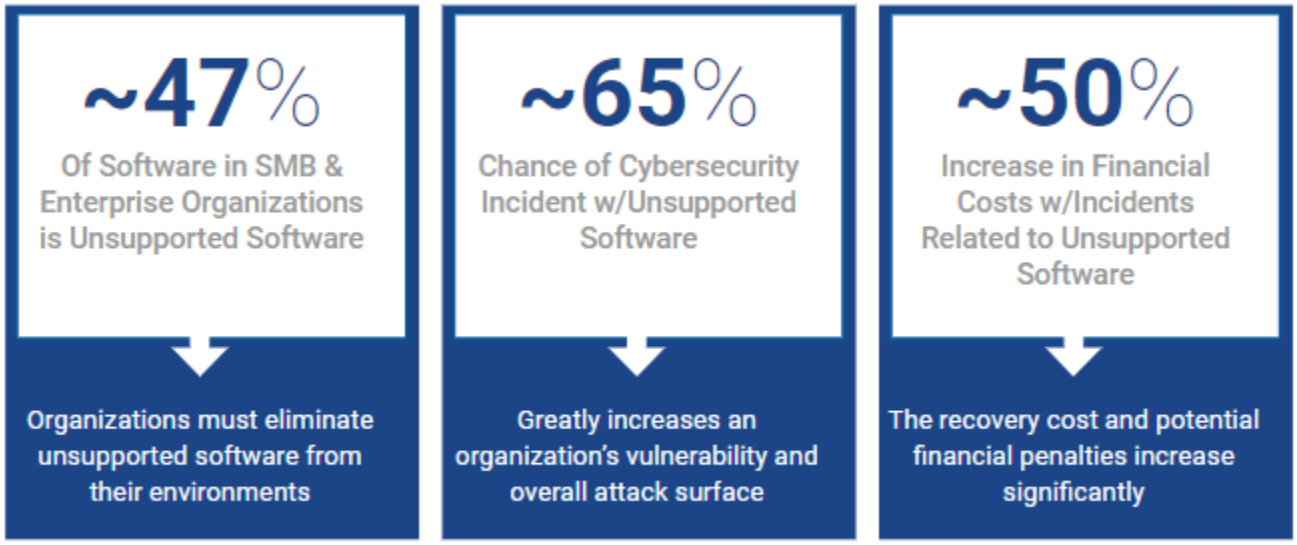


However, implementing a strong cybersecurity discipline can take some time and in the meantime, an organization is only as strong as its weakest link. This has never been more true when you consider the speed at which technology changes and the fact that the technology risk chain is often spread far and wide across an organization cutting across business functions, stakeholders and internal technology owners. Many risks are hidden from view lurking just below the obvious attack surface. An example of this is technical debt and in particular, **unsupported software**.

How does unsupported software impact your business?

A comprehensive Kaspersky IT Security Economics survey conducted in 2020 found that 47% of businesses still use some type of unsupported software. This is a concerning figure as the survey further showed that businesses with unsupported software have a 65% chance of experiencing a cybersecurity incident compared to a 29% chance for those businesses who keep their software updated. The survey also found that the financial cost of a breach, when unsupported software is involved, averaged 50% higher than breaches where this is not the case.

Cybersecurity aside, unsupported software or outdated software that is not maintained has an inherently higher risk level and probability of failure. As detailed in a January 2023 Forbes article, a painful and extreme example of this was the Southwest Airlines flight cancellation debacle that occurred in December 2022. The result was 16,700 canceled flights and an estimated $825M in financial losses. The root cause was outdated and neglected scheduling software.



Source: Kaspersky IT Security Economics 2020 Survey

Unsupported software may exist for many reasons in an organization. In the worst case, it is old "legacy" software with no readily available alternative and it is used to support a critical business operation or process. In the best case, it is a piece of software that is being managed via a software life cycle roadmap, has a known end-of-life date, has a viable software alternative already identified and a plan to implement. Like a standard bell curve, most software will likely fall somewhere between these two extremes which can be a bit muddy.

Given the above, it is easy to see how some software might quietly drift into an unsupported risk state. This is especially true of older software that has been performing well to-date or software that has been incorrectly deemed "non-critical." In other cases, it might be considered "non-production" receiving reduced levels of change management oversight in an effort to keep support costs down. This can be a slippery slope as you really have to take a step back and look through a wider lens and understand how that particular software supports an entire end-to-end business process and any cross functional dependencies. More importantly, organizations need to really assess the broader business implications of that software failing or not functioning properly.

Consider the following and ask yourself, what the operational business impact would be if:

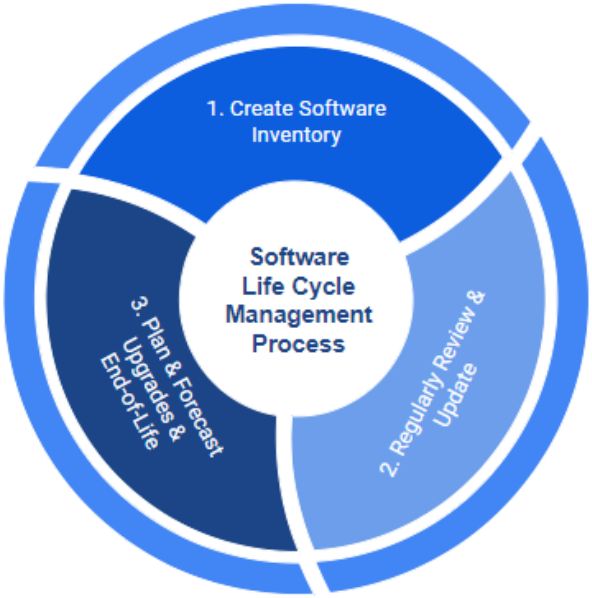
- The software was no longer maintained with bugs not being addressed?
- Internal software limitations created instability and performance issues?
- New security vulnerabilities were identified that cannot be patched?
- The underlying Operating System (OS) of the software needs to be upgraded but cannot be upgraded due to compatibility issues?
- The data associated with the software was corrupted or inaccessible?
- Business interruptions due to this software caused a compliance issue, fines or reputational damage?

What to do? Be proactive

The best way to avoid having unsupported software in an organization is to proactively manage the life cycle of all of the software that is used throughout the entire business. This includes having an effective software life cycle management process that establishes, maintains, and reviews the organization's software inventory. At a minimum, this software inventory will contain all pertinent information about the software such as:

- Vendor Name
- Vendor Contact Information
- Name of Software
- Business Purpose
- Business Criticality or Impact Level
- Data Classification
- Business Owner
- Technology Owner
- User or License Count
- Cost of SaaS Subscription or Licenses
- Date of Renewal
- Current Version
- Target Date for Upgrade or End-of-Life (EOL)

There are many software packages available to help technology leaders capture and maintain this type of software and configuration information. However, if nothing is in place today, a simple spreadsheet is a good place to start.



While this may seem very straightforward, many organizations fall short as the information becomes stale and is not used. Often, the software inventory gets created but is not well maintained and ultimately, cannot be used to drive future planning and budget forecast allocations. Given this, it is not surprising to see survey results indicating that 47% of businesses use unsupported software.

To be successful in managing the life cycle of software, organizations need to have a proactive software life cycle management process wrapped around this inventory information. One could argue that the process is more important than the software inventory itself. The need for this process is compounded as employees can easily obtain SaaS software without governance and oversight creating unintentional data leakage and unknown critical business process dependencies.

Conclusion

Given the rate of both business and technology change facing most organizations, it is clear that technology leaders are being challenged like never before to not only enable business operations but to also reduce cybersecurity and overall business risk. A natural inclination as technologists is to focus effort and budget on establishing strong cybersecurity capabilities. We can all agree that it is absolutely mandatory for things like infrastructure to be protected. However, it is not enough.

To truly address the full scope of risk, organizations need to look deep within and across the sprawling technology chain and related business processes to identify hidden weak links. One, if not many of those hidden weak links, will be found in unsupported software. If left unchecked or ignored, the outcome could really harm your business.