Is your legacy technology making you less secure?

Anyone introducing new technology into an organization can expect numerous questions from skeptical IT security professionals. After all, IT professionals have seen countless surveys and industry articles criticizing BYOD or cloud-based environments for their inherent problems in managing data security. Yet all the attention on new risks does not mean you can assume your data is adequately protected by the legacy technology operating in your organization. Software and devices that were once the secure workhorses of the organization can become old, unsupported and unpatched over time … in a word, risky.

Should you just get rid of legacy technology? Not necessarily — security isn't the only consideration for holding on to legacy technology. What you do not have, however, is the option of standing still. Organizations that stop maintaining systems that are still operational are leaving themselves vulnerable to attack.

Ask yourself these questions when exploring what to do with legacy technology and how to harden or enhance security measures for its continued life:

Is the old technology still supported by the original vendor?

When security patches and technical support are no longer available, this can lead to risk, especially over time. A system that is secure today can quickly become vulnerable as threats evolve and fixes to those vulnerabilities are not provided.

Are critical weaknesses for this old technology widely known?

Some technology was never very secure to begin with, such as applications that have a reputation for being full of security holes or extremely easy to exploit. If this is the case with your old technology, continuing to find ways to support it may produce more risk than reward.

Is it supporting or accessing sensitive or confidential information?

This seems like a no-brainer, but it often comes as a surprise when organizations decide to take a comprehensive inventory of old technology at just how much of it is accessing sensitive and critical data. Even worse, this is sometimes happening without the IT security team's knowledge or involvement.

When was the last time security patches were deployed?

Failure to deploy security patches can create a downward spiral that's difficult to bounce back from. We've seen cases where technology already scheduled for replacement just gets ignored in the interim because, after all, it's going to be replaced. However, when it ends up staying around for much longer than expected it can become a major security risk.

Is it a threat to compliance?

Some problems can, and should, be deal-breakers for legacy technology. Limited governance to enforce the requirements of internal policies, industry standards or regulatory controls is one of them. If the use of old technology is hindering uniform processes and procedures for the company, if it doesn't allow you to restrict user access, if you can't authenticate those who access the system or determine whether the data they are accessing is properly secured, then the only option is likely replacement.

If the outcome of your analysis is to keep the legacy system operational, it's important to keep in mind that evaluation must be an ongoing process — don't lapse into an "if it ain't broke, don't fix it" mindset. Even a small change in the surrounding threat landscape can make a system that you think is adequately secure today evolve into one that is not. Similarly, don't turn your legacy technology into a ticking time-bomb by waiting for a crisis to address exploited vulnerabilities.

Whether your legacy technology is on its way out or looks to be around for the foreseeable future, applying a regular, consistent and thorough IT security risk analysis will help your organization avoid potential pitfalls and maintain practical levels of security and control.

About Kroll

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services. Headquartered in New York with more than 50 offices across nearly 30 countries, Kroll has a multidisciplinary team of over 2,000 employees and serves a global clientele of law firms, financial institutions, corporations, non-profit institutions, government agencies, and individuals. For more information visit www.kroll.com.

These materials have been prepared for general information purposes only and do not constitute legal or other professional advice.
Always consult with your own professional and legal advisors concerning your individual situation and any specific questions you may have.

CONTACT

For more information, call or visit us online:
+1 866.419.2052

kroll.com

Kroll®