Info Snapshot, sponsored by DXC Technology | May 2024

Tech Debt Creates Cybersecurity Debt

Cybersecurity debt dramatically increases the chances of a successful cybersecurity attack.

Philip D. Harris
Research Director,
GRC Software & Services, IDC

Path to Reduction:
Tactical IT Creates Cybersecurity Debt, Alignment Between IT and Cybersecurity Reduces Debt

What Cybersecurity Debt Is Created from Technical Debt?

- Improper implementation and change control
- Unmanaged misconfiguration or configuration drift
- Minimal patching or updating
- Noncompliance to cybersecurity policies
- Lack of strategy IT and cybersecurity architectures

Rigorous IT Management and Cybersecurity Compliance Reduces Debt

- Align cybersecurity strategy and road map to IT and business strategies
- Add cybersecurity to systems development life cycle and change management processes
- Implement continuous compliance across the IT estate
- Identify, analyze, and incorporate/integrate shadow IT under corporate IT control
- Ensure continuous support from executives and the board for strategic direction of IT and cybersecurity

Tech Debt Increases Cybersecurity Debt

Tactical IT and cybersecurity programs can create rampant debt for both areas. This debt can expose the organization to potential cyberattacks and technology disruptions resulting from an out-of-control IT estate, technology portfolio bloat, risks, and unmanaged noncompliance deficiencies.

When IT and cybersecurity teams are tactical and unfocused and lack strategy, they run from issue to issue to acquire technologies to plug the holes. Such solutions could end up as “throwaway” expenditures within a short amount of time. They also create technology portfolio bloat, which leads to unforeseen risks, such as default configurations, misconfigurations, partial implementations, or too many technologies to manage.

The same is true when cybersecurity and IT teams are misaligned in strategy and direction. Cybersecurity will be busy mitigating risks as they arise, looking for a new tool or solution to deal with the latest vulnerability or cyberattack. The team will be seen as a business and IT inhibitor, and it will not be able to provide guidance to either department.

The business team is constantly pushing its agenda forward, looking for the next strategic decision to drive revenue and grow customer satisfaction. IT and cybersecurity often must play catch-up to provide controls and solutions to reduce risks. IT may end up taking budget and resources from other operational priorities, including cybersecurity.

Continue reading >

As a result, cybersecurity may implement less-than-adequate controls at the outset. This further erodes business trust that IT and cybersecurity are aligned with the business strategy.

Minimize Cybersecurity Debt Resulting from Technical Debt

To reduce technical debt and cybersecurity debt, organizations must transition IT and cybersecurity from tactical to strategic mindsets. Start by aligning cybersecurity, IT, and business strategies and road maps. This will offer:

- Visibility into and tighter control over technology spend
- Increased policy compliance
- Enhanced staff productivity
- Technology portfolio consolidation
- Improved change management
- Reduced business need for shadow IT
- Continuous maintenance of technologies
- Reduced cybersecurity risks and vulnerabilities

This approach also guarantees the new technologies are integrated into the IT estate properly.

Cybersecurity teams must be incorporated throughout IT management processes, systems development, and project life cycles. Doing so ensures that potential risks are identified and resolved prior to production implementation and technologies have appropriate ongoing security controls and documentation.

Another critical component will be to implement a continuous compliance monitoring solution that reviews and scans the IT estate for deficiencies such as improper security configurations, unpatched technologies, and unauthorized activities. This will translate into an ongoing reduction of risk, whether an issue is introduced by noncompliance with policies, configuration drift, or improperly implemented controls. All issues are dealt with immediately as part of IT's ongoing operational activities.

Finally, it is crucial that executive management and the board of directors support the strategic direction of IT and cybersecurity. Consider implementing cyber-risk quantification to accomplish this goal. When IT and cybersecurity leaders speak to executives and board members from a financial perspective, it is easier to garner interest and support for investments to reduce cybersecurity debt.

Message from the Sponsor

DXC TECHNOLOGY

While tech debt accumulation is continuous and inevitable, you can minimize the amount of debt that you accumulate, create strategies to address your current tech debt, and build an organizational process that limits the amount of future tech debt you create.

Reframe your technical debt

Produced by: IDC Custom Solutions
Info Snapshot, sponsored by DXC Technology | May 2024 | IDC #US52103624

IDC Custom Solutions produced this publication. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.