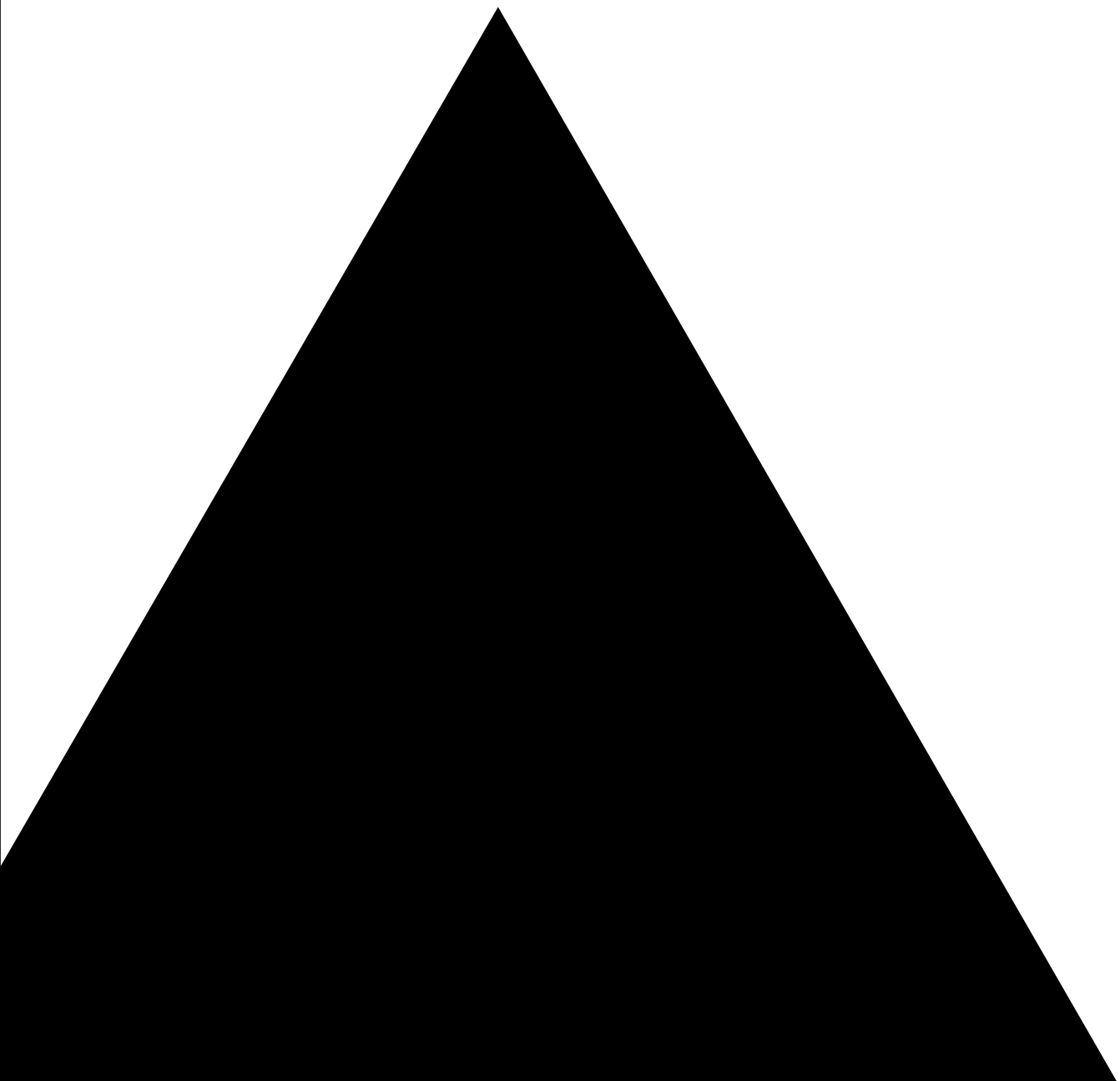
DXC.technology

Business white paper

The New Attack Vector: Applications

Reduce risk and cost by designing in security.



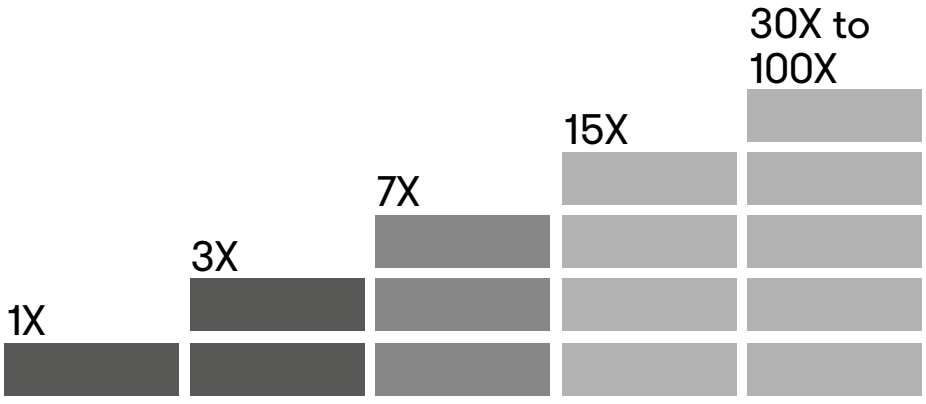
Is it Time to Reprioritize?

As cybersecurity threats become more mature, more focused, and more dangerous, companies and governments throughout the nation, and indeed, throughout the world, continue to struggle to provide an acceptable level of protection for their intellectual and physical property and the data they safeguard.

How much security is enough? This question plagues governments and businesses alike; clearly, there is no one right answer. Any breach resulting in exposure or loss of critical information is one too many. "Network/perimeter" security was the initial frontier for cybersecurity professionals. By and large, the level of protection that has been accomplished in this area has effectively thwarted most attempts at breaching the foundational layer of the cybersecurity protocol stack. Today, that is not enough. It is no longer practical to disallow almost all communications through the network layer. The attacker looks for the weak underbelly of IT and that is where we need to look, as well.

A security breach investigation report conducted by 7Safe entitled, "An Analysis of Data Compromise Cases 2010," identifies where attackers have recently targeted their efforts: 86 percent of the systems that were breached in 2010 were attacked at the Web Application layer, compared to only 14 percent of attacks that were aimed at the Infrastructure layer. The Microsoft Security Intelligence Report (Version 12) reinforces this conclusion by reporting that applications continued to account for the vast majority (greater than 70 percent) of all vulnerabilities in the second half of 2011.

Understanding and responding to the most common threat vector is the right start to implementing a more effective cybersecurity prioritization process.
The applications layer has been largely under-protected and it's now vital to strengthen our cybersecurity posture in this area. While organizations have to be vigilant at every layer, application security should be the "new normal" and at the forefront of every organization's cybersecurity defenses. Now is the time to take a proactive approach by engaging the adversary where they are attacking its biggest target ... applications.



Cost of Defect Repairw

Relative cost of defect repair depending upon when in the Software Development Lifecycle the defect is found and fixed.

Build In; Don't Bolt On

It is a well-established fact in software development that the earlier a defect is avoided, or discovered and removed, the more cost can be contained or reduced. Various studies have shown that software defects found and fixed after deployment will cost at least an order of magnitude more than if they had been found (or avoided!) at the beginning of the lifecycle. The National Institute of Standards and Technology (NIST) estimates it is 30 times or more expensive to "bolt on" quality after deployment. Barry Boehm, the inventor of the Spiral Lifecycle and who was also quoted in the NIST study, found a 100 times increase in cost when defect discovery and repair is delayed.

The Cost of "Reactivity"

In a very real sense, quality is a "pay a little now…or pay a lot later" challenge, but "later" can occur almost immediately in application testing or deployment. Delaying defect repair will increase exposure, risk, and costs. When the quality you are assessing is actually a cybersecurity risk, the stakes get very high. You can roll the dice and hope that your application won't be compromised, but you must be prepared for the cost of the breach which would typically represent an order of magnitude or more above what it would cost to find and fix the problem in the development stage.

Vigilance is more important than ever. Vulnerabilities, or security defects, are deficiencies that allow attackers to perform unauthorized actions and circumvent protection mechanisms. The cost of these vulnerabilities ranges from the risk in accomplishing the mission or business function and the risk to the brand and/or reputation, to the risk of data loss, or risk of delaying the software deployment. Once applications are in production, undiscovered vulnerabilities increase risk and costs requiring expensive software testing, updates, and patching.

Recent legislation, including the Ike Skelton National Defense Authorization Act for Fiscal Year 2011, increased the pressure on software security and quality with emphasis on:

- "assuring the security of software and software applications during software development," and
- "detecting vulnerabilities during testing of software."

This assumes defects are, or can be, discovered through normal testing procedures. Testing, which can only account for some known vulnerabilities, leaves previously unknown vulnerabilities exposed. The result is detecting security defects only after a breach has occurred.

The virulence and frequency of attacks today requires ever-increasing expenditures for remediation. The smart move is to review current security practices to include application development to ensure a "design security in" approach in software development versus the often practiced "bolt security on" approach that has been followed in the past. The "design security in" approach can actually reduce the total cost of development and operation of an application as well as provide enhanced, up-front protection against latent vulnerabilities.

The Proactive Approach

DXC Technology focuses on proactively improving security at every stage of the Software (or Systems) Development Lifecycle (SDLC). This means "architecting security in" from the beginning, with a laser focus on applications specifically within the architectural layer to avoid tens, hundreds, and sometimes thousands of vulnerabilities at a time. Often with a single architectural change or applying secure design principles, many vulnerabilities are eliminated or mitigated. This both improves security and reduces cost. Specifically, the DXC Comprehensive Applications Threat Analysis (CATA) Service can ensure cybersecurity is "built in."

The CATA service helps our clients identify critical yet missing security requirements in application development as well as those architectural choices that unnecessarily—and often dramatically—increase the number and severity of both known and unknown vulnerabilities. Using CATA, specific recommended actions are identified to address problems from both a regulatory perspective and an architectural threat model view. This service highlights activities in the earliest phases of the development lifecycle, the Requirements and Architecture/Design phase, but is also used to validate security resiliency for applications already in production. CATA differs from industry standard applications security methodologies by attacking the problem from a requirements and architectural viewpoint, which helps eliminate entire classes of vulnerabilities rather than just individual weaknesses in software that take excessive time and effort to remediate.

The best way to secure applications is to think cybersecurity "early on" as well as throughout the development lifecycle. Consider the following comparison of applications security methodologies: two nearly identical applications were developed, one utilizing the DXC CATA service and the other using traditional developmental approaches. The CATA process assessed and enabled the resolution of security requirements gaps and architectural security resiliency early in the process. The application that used CATA avoided over 70 vulnerabilities as a result of addressing a single finding, while the other methodology resulted in several patches and security bulletins to react to the same vulnerabilities after deployment. As previously mentioned, CATA findings can often avoid tens, hundreds, and sometimes thousands of vulnerabilities. The small, up-front investment in security quality improvement can pay for itself many times over in avoiding expensive, reactive security fixes and patching.

Review	Development		Release	Result
No Review	Security defects unknowingly introduced during development		70+ security defects needed to be fixed in postrelease security advisories creating high risk and high remediation costs.	Higher Risk & Cost
DXC CATA Review	Review during development phase avoided 70+ vulnerabilities.		Security defects fixed before release, reducing post-release risk and patch costs.	Reduced Risk & Cost

For More Information

The Optimized Approach

Developing a fully optimized cybersecurity approach requires a holistic viewpoint of applications security approaches that balance complementary processes and tools.

By designing security in and then augmenting with conventional application security approaches, all phases of the SDLC can be addressed and maintenance costs are reduced while increasing security.

This optimized approach combines secure architectural design principles, security code analysis or scanning, vulnerability assessments, and penetration testing to avoid, mitigate, find, or fix vulnerabilities as early as practical, resulting in fewer vulnerabilities to be addressed at the most expensive time – late in the development lifecycle. In a world of ever-shrinking budgets, increasing IT efficiency is one of the few ways you can cut costs. By utilizing a secure application development approach, the total cost of development/operation is reduced. This is an ideal way to cut costs while increasing security at the same time.

About the Authors

John Diamant, CSSLP, CISSP,
DXC Distinguished Technologist and DXC's Secure Product Development Strategist. He founded and leads the DXC security quality program, based on a foundation of building security into applications from the beginning, leads the DXC U.S. Public Sector Application Security Strategy, and leads the DXC CATA Service offering. John has extensive experience in the security development space including product development, security in the Software Development Lifecycle (SDLC), and security requirements and threat modeling. He's experienced in all phases of software development and leadership, and is a prolific inventor with seven issued patents and several more pending.

Jeff Misustin
A DXC Marketing leader nd brings more than 20 years' experience in the computer technology field in the public and private sectors. Jeff has a breadth of experience focusing primarily on application services but has experience in managing all facets of IT delivery. He has worked within complex environments —bringing innovative solutions to provide comprehensive successful outcomes for clients.

Learn more at www.dxc.technology /applications

About DXC
DXC Technology (NYSE: DXC) is the world's leading independent, end-to-end IT services company, helping clients harness the power of innovation to thrive on change. Created by the merger of CSC and the Enterprise Services business of Hewlett Packard Enterprise, DXC Technology serves nearly 6,000 private and public sector clients across 70 countries. The company's technology independence, global talent and extensive partner alliance combine to deliver powerful next-generation IT services and solutions. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.

© 2017 DXC Technology Company. All rights reserved.

DXC_AA4-3092ENW. March 2017