Innovating Resilience

Innovation is not just about new products, new ways to compete and developing new features. Innovation is also examining what is in place today, seeing where the gaps are and building solutions to address those gaps. When it comes to resilience, innovation has a strong role to play.

Using Existing Technologies in New Ways

We have a myriad of technologies that allow us to keep IT operations available in the face of issues and failures. Much of the time, we can implement something we already know and are familiar with to ensure that operations are either uninterrupted or recovered quickly (based on business requirements). For instance, proper, timely backups can help an organization recover from a ransomware attack even if the organization suffers from an initial outage of some or all services. While backups were not designed to counter ransomware, ransomware leads to the same result: destruction of data and/or systems. Therefore, it makes sense to use the tried and true technology of backups as a layer in our defenses. This is using an existing technology in a new way.

K. Brian Kelley, CISA, CSPO, MCSE, Security+
Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

Embracing New Technologies

Part of being innovative is looking beyond the tried and true. So in addition to considering what we know and understand well, we always need to expand into improvements in existing technology and new classes of technology.

For instance, once upon a time, replicating data from one data center to another was a difficult proposition. However, improved storage area network (SAN) and network-attached storage (NAS) technologies means solutions are easier to deploy. Clustering technologies have improved greatly, especially across sites, with new features and approaches that often take advantage of the advancements in storage. Then there is the impact of the cloud itself, which represents a new class of technology. Cloud vendors look to build offerings that provide recovery and availability options for customers, whether they are operating completely in the cloud or have a hybrid approach. At the rapid pace at which new technology is developed, we will likely never run out of new technology to consider.

Thinking Outside of the Box to Discover Issues

We are not just applying technology to keep busy. We deploy solutions to solve problems. As we discover issues, we should have answers.

In incident response, we often perform vulnerability scans to check for issues. The limitation with vulnerability scans is that they detect known issues such as default configurations, widely occurring misconfigurations, missing patches and standard weaknesses such as cross-site scripting or Structured Query Language (SQL) injection vulnerabilities. To dig deeper and find new vulnerabilities, we use techniques such as penetration testing. For instance, recently a security researcher was able to find a *chess.com* vulnerability by looking at the returned JavaScript Object Notation (JSON) response.[1] From the data, he harvested the security token and logged in as an admin. A vulnerability assessment tool by itself would not have been able to connect the dots. To find the vulnerability, the researcher had to put creative thinking into play to see the potential for the vulnerability. Once he did so, he was able to test this potential hole and prove that it existed.

Admittedly, penetration tests tend to be expensive and focus primarily on cybersecurity. Something cheaper and less specific is the tabletop exercise. By putting the right people around a (virtual) table, we can walk through a system and look at various issues that might arise. By walking through the steps by which a system deals with those issues, we can find problems in our configuration/implementation. Also during these exercises, new questions come up that may lead to the discovery of an issue no one had considered before. Through this exercise and others like it, we can uncover additional resilience issues in a given system.

Learning From Outages

However, the reality is that in large, complex systems, we are still likely to miss some issues. Then there are cases when outside events (e.g., natural disasters) go beyond what we typically consider. To avoid a repeat, we must learn from our failures.

For example, in February 2021, both Hyundai and KIA reported lengthy IT-related outages that affected operations, especially in the United States.[2] Considering that KIA's outage affected US dealerships and more than likely impacted sales, we would expect after recovering from outages that both organizations will investigate thoroughly. Any time we see an outage of that scale, we can expect that the organization will perform a root cause analysis to prevent such a repeat occurrence. Oftentimes that investigation reveals a number of issues, all of which need creative solutions because the issues were either more complex than previously thought or were not understood to exist. After all, in almost every case, the organizations experiencing such outages had done a great deal of planning and designing for resilience, but something still went wrong. This is where innovation comes to the forefront.

Learning From Complex System Issues and Unexpected Single Points of Failure

A classic example of this type of investigation happened after the large-scale Microsoft Azure and Office 365 outage in September 2018.[3] Lightning strikes impacted cooling systems and the loss of those cooling systems resulted in an automated data center power down. To this point, everything was according to plan. However, while Microsoft cloud architects engineered for resilience, they missed some issues because of the complexity of the services. For instance, some services, while provided across multiple regions, had one or more components that existed only in the region with the downed data center.[4]

Beyond the obvious Azure offerings, there were also multiregion issues in other services, such as Office 365. Here, rerouting Azure Active Directory (AAD) due to the downed data center caused automatic throttling to kick in for other sites, resulting in extended login times and login timeouts. All of these services share that same login mechanism. This revealed another unexpected problem: A resiliency protection for Azure AD actually worked against resilience.[5]

In Microsoft's case, there was a technology that it had developed for its cloud operations called Availability Zones.[6] Availability Zones are designed to protect against a data center failure such as what was experienced. However, at the time of the failure, Availability Zones were not yet available in the region that experienced the failure. Microsoft had existing technology that could have prevented the outage. It was just a matter of getting it implemented.

Learning From Outside Events/Natural Disasters

We also have to consider outside events and natural disasters with respect to outages. For instance, the COVID-19 pandemic is an outside event that few organizations anticipated. Effectively overnight, a large number of organizations had to shift to remote-only without the proper setup and planning. Even service providers such as those offering virtual

Enjoying this article?

- Read *Managing Security Impacts in a Multicloud Environment. www.isaca.org/multicloud-security-impacts*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> “SOMETIMES, NEW IDEAS THAT SEEM OUTLANDISH WHEN FIRST PROPOSED TURN OUT TO BE BETTER SOLUTIONS THAN WHAT WE HAVE.”

team and meeting services—providers who had designed their infrastructure for scalability—found themselves overwhelmed by the usage and suffered capacity issues. The good news is that many organizations were able to make the transition, albeit with some hiccups, and did so in rapid fashion.

However, in the case of the pandemic, the physical infrastructure for organizations is still intact, whether that sits in their owned/leased data center space or in the cloud. Other disasters have not been as kind. For instance, when Hurricane Katrina hit the Gulf Coast of the United States, many organizations in that region had no power to their data centers at best. At worst, they suffered physical equipment and facility damage. We must have solutions in place to handle these situations, too. Here is where the cloud becomes an attractive solution.

Innovation Can Mean Accepting Unusual Solutions

Sometimes no current technology addresses a particular issue. In other cases, there is technology that does, but it is too expensive. A third possibility is the solution has too many limitations. An innovating solution may overcome all of these obstacles.

Thinking outside of technology, likely many people never thought we should manage a major software development effort using a whiteboard, Sharpies and Post-It Notes. However, participate in a Scrum stand-up and that is what you will see, though those materials tend to be virtual now due to the pandemic. Along those lines, with the crippling cold and the extended loss of power that hobbled the US State of Texas, one man posted that his Ford F-150 with onboard Pro Power generator was powering his essentials. As a result, Ford asked dealers to loan their trucks so residents could have access to electricity.[7] It is unlikely that anyone had the Ford F-150 on their list of how to handle an extended power outage. However, it is a solid, easy-to-implement and relatively inexpensive solution.

Similarly, when we face resilience challenges, our teams may develop unusual solutions. As long as they are sound and address the problem properly, the proposed solutions should be considered. Sometimes, new ideas that seem outlandish when first proposed turn out to be better solutions than what we have. Agile and its associated methodologies are a great example. Since they work, they have stuck around while other methodologies have not. That is how we should approach innovative ideas to improve resilience.

Endnotes

[1] Sotnikov, D.; “API Security Weekly: Issue #121,” DZone.com, 17 February 2021, *https://dzone.com/articles/api-security-weekly-issue-121*

[2] Bajak, F.; “Kia and Hyundai Recovering From Days-Long Network Outages,” AP News, 19 February 2021, *https://apnews.com/article/smartphones-us-news-6cb4c59483e24cac3758079e3c8d7bb1*

[3] Mackie, K.; “Microsoft Azure and Office 365 Services Go Down in Texas Service Area,” *Redmond Magazine*, 4 September 2018, *https://redmondmag.com/articles/2018/09/04/azure-office-365-down-in-texas.aspx*

[4] Hodges, B.; “Postmortem: VSTS 4 September 2018,” Azure DevOps Blog, 10 September 2018, *https://devblogs.microsoft.com/devopsservice/?p=17485*

[5] Mackie, K.; “Microsoft Explains Sept. 4 Service Outage at Texas Datacenter,” *Redmond Magazine*, 11 September 2018, *https://redmondmag.com/articles/2018/09/11/microsoft-explains-sept-4-outage.aspx*

[6] Microsoft, “Regions and Availability Zones in Azure,” 9 April 2021, *https://docs.microsoft.com/en-us/azure/availability-zones/az-overview*

[7] Yekikian, N.; “Ford Asks Texas Dealers to Loan Out F-150 Hybrids to Serve as Home Generators,” *MotorTrend*, 19 February 2021, *https://www.motortrend.com/news/ford-f-150-generator-dealer-loan/*