Cybersecurity Is Still Critical

There are a great many things that go into digital trust and a digital trust ecosystem, but a core component is still cybersecurity. How good is an organization's cybersecurity reputation? Does it have any known breaches? Were any of those breaches extremely bad, either because of impact to the business (and loss of product) or the loss of customer data? An organization's digital trustworthiness is influenced by a number of factors that are not cybersecurity. Organizations should be concerned about their brands and overall reputations. They need to increasingly improve relationships, both with third parties and customers. They must ensure that their abilities to execute and deliver meets expectations. However, the reality is that a poor showing on the cybersecurity side could impact all of those things.

K. BRIAN KELLEY | CISA, CDPSE, 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.

Cybersecurity Is Still Important Up and Down the Chain

Earlier this year, the big news in information security was GoDaddy's multiyear breach.[1] What GoDaddy shared was alarming: It did not know who the attackers were; customer and employee credentials were stolen, and attackers were able to install malware that caused legitimate sites to redirect to malicious ones (watering hole attacks). At the time of this writing, the size of the impact to GoDaddy and its current customers is unknown. How many will leave? The current customer base is approximately 21 million, with 2022 revenue of approximately US$4 billion.[2]

The details about what was breached and how it was breached, along with the duration of the compromises, are alarming. While GoDaddy may have had robust cybersecurity assets in place, they were obviously not enough. This not only damages GoDaddy's reputation, but also potentially damages the reputations of customers who relied on GoDaddy for hosting, such as through the GoDaddy WordPress hosted solution. After all, if customers go to an organization's GoDaddy-hosted site and are redirected to and infected by a malicious website, it still appears that the organization's site is the one that caused the compromise. Its customers are not likely to trace the problem all the way to an issue with GoDaddy. Even if they were technically savvy enough to do so, they likely would not have the time—or they may not care enough about how it happened.

When LAPSUS$ claimed a hack of Okta in 2022,[3] many in the information security world took notice. More important, current and potential customers paid attention. The truth of the matter was that Okta itself was not directly hacked. Rather, an outsourced call center provider was the target, and that allowed LAPSUS$ to get access to Okta customers. The overall impact to Okta customers was small—only 2.5 percent were affected. However, the news of the hack stayed in the industry press for weeks and it is likely that some potential customers were dissuaded from using Okta and some existing customers chose to migrate to other providers. At the end of the day, it did not matter that Okta was not the direct target. This is a great example of potential and current customers losing trust in an organization due to a problem with a third party.

The cybersecurity strength of one's organization is important. GoDaddy certainly will suffer a reputation hit, that will lead to lessened trust in its brand and that will almost certainly cause it to lose customers. However, some of GoDaddy's own customers probably have lost customers themselves in the face of the breaches GoDaddy suffered. It is likely that Okta has lost customers because of the breach of a third-party call center due to weakened trust in its brand.

When it comes to using the cloud, it is important to remember that there is a shared security model, meaning security is not the sole responsibility of the provider.

Using the Cloud and Its (Lack of) Impact on Digital Trust

This is almost a click bait-worthy subhead, but it is important to note that if an organization is using a cloud-based resource and there is a security issue, the fact that it is a cloud-based resource does not seem to have much in the way of impact vs. an on-premises resource.

Again, it is worthwhile to look at Okta. It suffered another breach, which came to light in December 2022. In that case, Okta code repositories hosted on GitHub were breached and Okta's source code for one of its product lines was copied.[4] There are no public details about how the threat actor gained access to the repositories. Even if there were, the fact remains that all the scrutiny and responsibility once again fell on Okta.

The fact that Github was cloud-based was not cited in the news articles about the breach, except as an education point for those who were aware of Github. Therefore, it appears that was Okta's use of a cloud-based code repository was a nonfactor in the impact to Okta's brand. Using cloud-based resources is an expected practice nowadays and, for the most part, is not treated any differently than if the resources are on premises. In actuality, Okta's services are built on top of Amazon Web Services (AWS)-provided functionality, meaning they are entirely cloud-based.[5] Returning to GitHub, if there were a weakness in GitHub's implementation, Okta's customers likely would not care for the same reason customers of organizations breached because of GoDaddy would not care.

To be clear, Okta is not the first organization to suffer a breach of a cloud-based resource and it certainly will not be the last. The organization proves to be an interesting case study because its breaches were recent and, especially with the LAPSUS$ hack, it had a weakness the industry probably had not considered seriously until it happened to Okta. When it comes to using the cloud, it is important to remember that there is a shared security model, meaning security is not the sole responsibility of the provider. One would expect the provider to handle physical security, for instance, but the provider cannot prevent a customer from implementing a poor identity and access management (IAM) model, which could lead to a breach. The customer side is certainly a weakness in the shared security model. Maybe it is because cloud computing is still a murky concept to too many IT professionals, but a number of organizations moving to the cloud struggle to properly secure resources. For instance, a study from 2020 found a large number of improperly secured AWS S3 storage buckets.[6] Since that study, media reports of yet more organizations, both private sector and government, have continued to come out regularly.

Which begs the question: Does cloud matter? No, it does not. In a nutshell, customers and potential partners do not care where resources are located. They care that they have been breached. It is not about cloud vs. on-premises anymore. It is simply about whether an organization's cybersecurity/information security posture is sufficient to cover its resources.

Do Some Organizations Have (Partial) Immunity?

Some organizations do have at least partial immunity from incidents that result in a loss of trust. Usually, these organizations are in niche markets or are so positioned that their customers and partners have no other choice but to deal with them. For instance, in an article reflecting on the Colonial Pipeline ransomware attack, the only cited numbers with respect to US

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums* dollars are the original amount that was paid and the amount recovered.[7] There is no conversation about loss of customers or loss of reputation. After all, the Colonial Pipeline does not have competitors in the sense that GoDaddy or Okta do. Even with a loss of trust, some organizations will not see an impact to their bottom lines.

However, the majority of organizations will see that digital trust is increasingly important. If I cannot trust an organization, I am not going to do business with it unless I have no other choice. As a partner, I do not want the factors that led to the organization's poor reputation to impact my reputation. As a customer, if I have a choice between two providers, unless there is something compelling that causes me to give the less trusted organization a chance, I am going to go with the more trusted one. One of those compelling factors could be a significant cost difference. But that means the organization in question makes less from any transaction with me. Therefore, it is important to the organization's bottom line to increase its trustworthiness.

Do Not Forget About Cybersecurity

Colonial Pipeline may not have lost customers, but because of its cybersecurity posture, it did lose millions of US dollars in the ransom payment alone. So, while it had partial immunity, it was just that: partial. Even an organization that does not rely on digital trust needs to ensure its cybersecurity is up to snuff.

For most organizations, cybersecurity posture is crucial to overall digital trust and impacts how partners and customers (and potential partners and customers) view the organization. The example of GoDaddy likely losing customers because of the announcement of the breach, along with the expectation that Okta will lose some customers, are based on such outcomes happening repeatedly.

Multiple studies by different organizations show the same findings: Data breaches lead to a loss of trust and, therefore, a loss of business. For instance, a PricewaterhouseCoopers (PwC) report[8] found that 85 percent of consumers would not do business with an organization if they were concerned about the organization's (cyber)security practices. Quite simply, cybersecurity cannot be neglected. Other aspects of the digital trust ecosystem are important, but they can all be undone overnight by a single data breach. Cybersecurity is not all there is to digital trust, but it is a key component that should not be ignored or undervalued.

> Cybersecurity is not all there is to digital trust, but it is a key component that should not be ignored or undervalued.

Endnotes

1 Goodin, D.; "GoDaddy Says a Multi-Year Breach Hijacked Customer Websites and Accounts," *Ars Technica*, 17 February 2023, *https://arstechnica.com/information-technology/2023/02/godaddy-says-a-multi-year-breach-hijacked-customer-websites-and-accounts/*

2 *Ibid*.

3 Brewster, T.; "Okta Hack Exposes a Huge Hole in Tech Giant Security: Their Call Centers," *Forbes*, 23 March 2022, *https://www.forbes.com/sites/thomasbrewster/2022/03/23/okta-hack-exposes-a-huge-hole-in-tech-giant-security/*

4 Okta, "Okta Code Repositories," 21 December 2022, *https://sec.okta.com/articles/2022/12/okta-code-repositories*

5 Okta, *Not All Cloud Services Are Built Alike*, USA, 2022, *https://www.okta.com/resources/whitepaper/not-all-cloud-services-are-built-alike/*

6 Nichols, S.; "Leaky AWS S3 Buckets Are so Common, They're Being Found by the Thousands Now—With Lots of Buried Secrets," *The Register*, 3 August 2020, *https://www.theregister.com/2020/08/03/leaky_s3_buckets/*

7 Henriquez, M.; "Reflecting on the Anniversary of Colonial Pipeline Ransomware Attack," *Security*, 9 May 2022, *https://www.securitymagazine.com/articles/97578-reflecting-on-the-anniversary-of-colonial-pipeline-ransomware-attack*

8 PricewaterhouseCoopers, *Customer Intelligence Series: Protect.me*, USA, 2017, *https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/protect-me/cis-protect-me-findings.pdf*