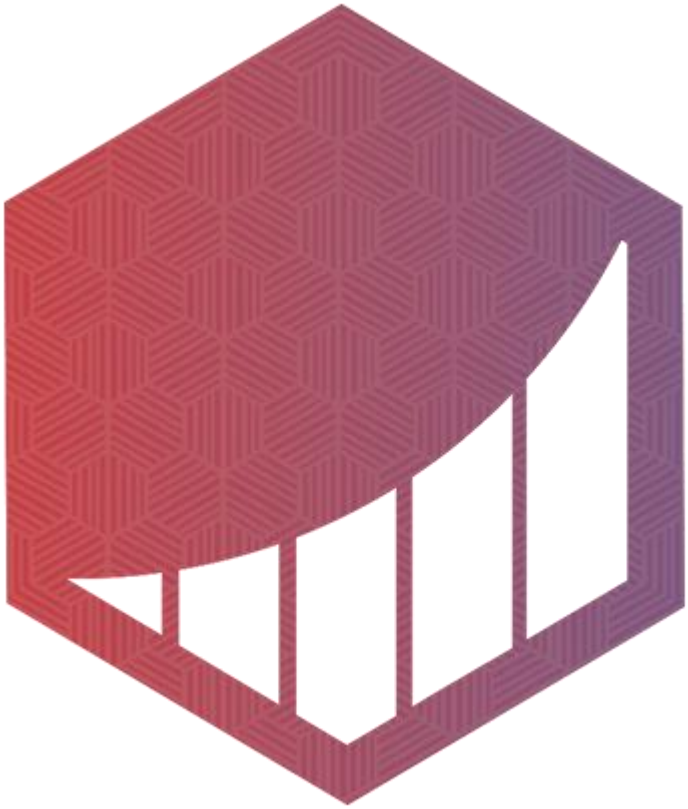

BRICK BRIDGE CONSULTING

Information Security Infrastructure at a Software Start-Up

CALEB HAYDEN
BRICK BRIDGE CONSULTING, LLC
600 ENVOY CIRCLE, JEFFERSONTOWN KY, 40299

Table of Contents

Executive Summary

Brick Bridge Consulting serves the governmental and nonprofit sectors of the greater Louisville area and beyond by providing CRM and business management solutions that are affordable and custom-built to meet client needs. In this short examination, we will analyze the aspects of the core tools that they use to do their work: Podio and Amazon Web Services. We will take a deep dive to discuss the security implications of these platforms and what it means for Brick Bridge as well as the clients who use these systems every day. We will also examine the physical security measures as well as the policies and behaviors of employees at Brick Bridge, to better understand how security impacts their workflow, as well how it may create a risk to the company. Following that, a brief set of recommendations will be offered as a means to improve on the vulnerabilities that may be identified herein.

In summary, the platforms utilized by Brick Bridge employ rigid security procedures and practices that help maintain both the integrity of the data within as well as the reliability of the systems as a whole. The Podio and AWS platforms make a good pair because they are highly scalable and can be adapted for use around the globe. Both platforms are inexpensive to the end-user and offer a robust amount of control to administrators and creators alike. As a result, the bulk of security vulnerability at Brick Bridge Consulting lies in the physical security of the workplace as well as the potentially dangerous behaviors and levels of access that employees gain by working on their projects.

Background

Brick Bridge Consulting, LLC[i], (which may also henceforth be referred to as "Brick Bridge Consulting", "Brick Bridge", or "BBC") is a Louisville-based local software development start-up, which at the time of writing, has a small but dedicated team of 9 people. Brick Bridge specializes in project-based work for clients that need business management solutions. Brick Bridge typically works with organizations in the non-profit and government sectors of Kentucky and the surrounding area but doesn't exclude work in the for-profit business market. Brick Bridge has clients large and small, ranging from Louisville Housing and Urban Development to local foster homes and even venture capital firms.

To meet the needs outlined in their contract-based work, Brick Bridge relies heavily on the utilization of Podio[ii] platform, a widely-used Customer Relationship Management System(CRM), and a direct competitor to the more commonly known platform SalesForce. At its core, Podio is a software for creating for creating forms using a drag-and-drop interface, which, when filled out by a user, populates a record in an easily manageable database. Users have granular control on exactly what fields and key performance indicators (KPI) that they wish to track for their business needs, as well as having easy control on how tables are related to one another. To make this as user-friendly as possible, Podio calls tables "apps" and users have control of what each app contains and how apps relate. Each user or organization can create and manipulate their own set of apps to fit their needs.

Podio also offers a complementary service called GlobiFlow[iii], which allows developers to create dynamic automations for users within Podio. For example, when a user clicks a submit button on an item in an app, an audit may run to check that required fields contain the information they need, and if not, relays feedback to the user. GlobiFlow uses the flexibility of

PHP notation, hidden behind a drag-and-drop interface, that allows for complex functionality within Podio. For smaller-scale projects, this is often the full toolset that Brick Bridge will employ to meet the needs of a client.

For projects of a larger scale, Brick Bridge has a team of developers, who primarily utilize .NET, who can create more complex functionality. In most cases, the bulk of this work is in developing services and functions that are stored and executed with Amazon Web Services(AWS)[iv] to deliver complex functionality that GlobiFlow cannot handle on its own, or at least, it can't do efficiently.

Lastly, Brick Bridge Consulting integrates consulting services into their core business model by working with clients to offer strategies and practices to get the full potential out of the solutions that Brick Bridge provides as well as advice to ensure business longevity and success. Brick Bridge also provides standalone consulting services for those who do not have other technical needs.

Security Overview

To maintain the safety of the clients and the company's assets, companies often employ a complex security infrastructure. In recent years, information security has become an increasingly important factor in a business's dealings. As technology continues to grow and evolve, people have begun to rightfully worry about their privacy and its potential misuse. Tech companies have also become valuable targets to cyberterrorists and all manner of hackers in recent years, presumably because their products and services have a diverse, global client base, and as such, are likely to have large amounts of sensitive client data in storage. No firm has proven to be completely immune, with even some of the world's largest companies being successfully

attacked in recent years, such as the CCleaner Malware Attack[v] in 2017. Attacks and exploits are more-or-less inevitable, and to combat these issues, the role of cybersecurity in the workplace has had to evolve to stay ahead of would-be attackers.

The purpose of the following document is to analyze the role and implementation of cybersecurity, as well as physical security, in the context of Brick Bridge Consulting. An analysis of the policies, practices and behaviors of it's employees will offer a glimpse into the strengths (and weaknesses) of the infrastructure that is employed by the company. It will take a brief look at how the information security infrastructure is evolving at BBC, as well as what direction it is moving toward. Lastly, this analysis will also serve to offer recommendations on how to address the weaknesses described throughout by applying the teachings of Dr. Andrew Wright's Introduction to Information Security course at the University of Louisville.

Podio: Security at the Platform Level

As mentioned in Background section, the core of all work at Brick Bridge is done using the Podio platform. It is trusted to be used for internal human resources and project management purposes and it allows for robust CRM systems for clients. Fortunately, Podio also boasts enterprise-grade security that is baked into every single user's account. Podio actively protects user data in several ways: by storing on-site backups as well as an off-site AWS cloud database, by using "Advanced Encryption Standards (AES) on all files", and by allowing access to the system "only with Secure Sockets Layers (SSL) connections". Podio is also "compliant with the U.S. - E.U. and U.S. - Privacy Shield compliance framework and conforms to ISO27001 security

policies."[vi] ISO27001 "is the best-known standard in the family providing requirements for an information security management system".[vii] This standard is technology-neutral, and as such, can be applied to any kind of business. Podio also hosts a publicly available document called White Paper[viii] which further details the system's security protocols.

ISO 27001 defines a six-part planning process:

1. Define a security policy.
2. Define the scope of the ISMS.
3. Conduct a risk assessment.
4. Manage identified risks.
5. Select control objectives and controls to be implemented.
6. Prepare a statement of applicability.

Podio user-level security features allow the administrator of any Podio system to control access on a granular level, all while maintaining a simple user interface. This means that within a system, an administrator can grant individual privileges to users, allowing them access and visibility to only the things they need to see to complete the functions of their job in the system. Users can only access apps and workspaces (collections of related apps) that they have been explicitly given access to view. Administrators can also allow or restrict several core Podio features as necessary, including, but not limited to, the ability to modify an app, the ability to modify or delete records in an app, the ability to modify the layout of an app, or the ability to create and delete apps.

It is also important to note that Podio offers several different tiers, with different user options. For example, in most pricing plans, organizations that utilize Podio pay for it on a monthly per-seat basis. However, Podio is flexible enough to allow for free accounts for external users in various situations. It also supports multiple using the same account at the same time, which is useful for several reasons. Each paid user has a unique login that they must individually set up, but free users, who have lower level access, may share an account that has only the privileges necessary to support low-level job functions. This allows Podio to scale with different

sized businesses but can also raise some security concerns if abused. If multiple users are on the same account, naturally they will have the same privileges and access to their Podio installation, which if a user manages to access an account maliciously, could case damage to that installation by manipulating data, changing other users' privileges, or by deleting apps altogether depending on the account the accessed. While this seems to be the most easily identifiable security concern of the Podio platform, the issue of account sharing, leaking and abuse is a general information security issue that has existed far longer than Podio has, and is not a weakness specific to this platform. In reality, the organizations that use Podio and experience this type of malicious behavior are at fault themselves, due in part to having non-comprehensive security policies and practices that could've helped prevent password sharing and the damage it caused in the first place. Ultimately it is up to the organization to determine a best approach when deciding when and if a shared account should be used for their purposes. If so, security privileges should reflect this choice, and lessen the possibility of abuse.

1. Software Security at Brick Bridge Consulting

1.1 Podio Security Measures

As previously mentioned, Podio serves as the basis for many internal functions at Brick Bridge. Gil Roberts, Partner and Director of Client Services, uses Podio to track a variety of employee functions at Brick Bridge. The Human Resources space allows employees to track their work hours and bill them to the specific project that those hours were spent on. This allows for simplified payroll and jointly allows him to see who is working on what at any given day. The space was carefully designed so that, while employee time punches are public, much like they would be at a traditional timeclock, important financial information such as hourly wage and paycheck amount are not visible to anyone except Gil. This space also features a calendar

page where business closings are listed, and employee sick day/time off requests can be easily made and reviewed.

The Project Management space allows Gil to create records of current projects and attach any necessary documentation to them, such as contracts, service-level agreements, non-disclosure agreements, and project proposals. From there, he can allow specific employees to have access to the record that pertains to a project that they are working on, if they need to review the documentation. This space also allows for progress tracking in the form of milestones (more granular tracking is done using the JIRA[ix] platform).

Only when an employee has been added to a project do they gain access to any workspaces, apps, documentation, etc. that exists in Podio for that project. Prior to deployment, a client's Podio workspaces are accessible by a Brick Bridge Service Account, controlled by the partners of BBC, which has the ability to add employees to the spaces they need to work in. Sometimes, employees work directly through the service account. Typically, when a project is deployed to the client, this service account retains access and, and serves as the entry point for administrative functions. Individual employee accounts are then removed from these workspaces, as they become redundant. This practice prevents clients from making changes to their installation that could otherwise break or manipulate functionality in a way they likely could not have foreseen. This also allows Brick Bridge employees to retain a point of entry into the workspaces to make quick iterative changes per the request of the client once the product has been deployed. Depending on the project, the client may maintain an administrative role. In these cases, Brick Bridge will create the administrator account and retain its credentials, then will securely share them with the appropriate member. Like the service account, this allows employees to retain access to the system to do their work, but also allows the client to have

administrative privileges. This is a somewhat rare set-up for Brick Bridge and typically only occurs in contracts where the client is retaining ownership of the solution that is being/has been developed.

The Brick Bridge Service Account can also be cited as a security weakness for the company and its clients. Typically, once a project has reached completion, the service account is removed from the associated workspaces. This means that Brick Bridge no longer has any access to that client's Podio installation. At any point, if a client requests service or assistance, that user will have to manually grant access to the service account using Podio's "invite" system. This is good, but this practice is not always enforced. Sometimes the service account lingers in client projects long after they have been deployed. Furthermore, during the entire duration of a project, this account is a guaranteed point-of-access to that client's installation. This means that a malicious user with access to the service account, could cause damage to any number of clients, some of which may already have live data in their Podio installations. This could cause a severe backlash in the relationship between Brick Bridge and the client, and since Podio doesn't offer any kind of data retrieval, if the client doesn't have a local data backup, the damage caused by the malicious user could be permanent and far-reaching.

This sort of behavior has never occurred at Brick Bridge, and hopefully never will, but this is a cause for concern, because nearly all employees have access to the service account given the nature of their work. To lessen the potential for abuse, more care should be taken to ensure that the service account is always removed from a client installation following its deployment. This issue could be further mitigated by allowing only the partners to control access to the service account, and requiring employees to use their own accounts to do the work required within a client's installation.

1.2 Development Security

For projects that require functionality that Podio and GlobiFlow cannot provide on its own, a team of developers use a variety of tools to create, host and store their work. Each developer uses their own installation of Visual Studio, and contributes their work to private repositories that are hosted on BitBucket[x]. Alex Shull, lead Software Engineer, uses myGet[xi] to host an array of custom, private NuGet packages that allows the team to more easily interact with the Podio API. By using myGet instead of NuGet, he can more easily make the packages private, and not searchable within Visual Studio Package Manager. Access to these services initially requires only a basic username and password. In the case of BitBucket, a team member can login, grab the link to clone a repository, and then access it indefinitely through the Visual Studio Team Explorer. MyGet works very similarly, a user can login and grab the link to subscribe to a myGet feed, and then can access that feed by adding it to the Visual Studio NuGet package manager. From there, it will pull updates to the subscribed packages as Alex pushes them, much in the same way that NuGet works.

The functions that the team writes are typically hosted as Lambda functions on AWS, which can operate asynchronously and are called with webhooks that the team can implement in Podio apps. When a developer writes a Lambda Function, there are special procedures that must be accounted for. Alex wrote an authenticator services that operates fundamentally by generating Podio OAuth tokens only when necessary. When a function is called, it must be authenticated by the Podio API before it can execute, and it hands in the OAuth token as a way of doing so. If the function attempts to authenticate and the token is expired, Alex's service will wipe the expired token and call to Podio for a new one. Then, it passes it to the function being called. After the

function is called, the OAuth token is stored in the Cloud by the service until it is requested again by a function.

In order to pass the token from the service to the function, we use environmental variables. Sometimes these variables may be constant across a variety of functions, such as a link to the API gateway, but instead of hard-coding it into each function where a would-be hacker could easily find it, we use environmental variables. Where the variable would be hardcoded, we instead define the variable inside the function's settings on AWS. When the function is called, it looks to Lambda to retrieve any environmental variables that it needs to execute. Developers take care to make sure that any critical sensitive information is stored as an environmental variable, from client identifiers to proxy server gateways. As such, each function may have several of these variables that it needs to operate fully. When a function is ready to be pushed to AWS, the user must user his Command Line Interface(CLI) which must have the Amazon CLI extension installed.

Access to AWS is limited to members of the development team, who had their accounts and permissions set up explicitly by Alex. Login requires the user to authenticate with username and password, followed by a code provided by the Google Authenticator mobile app. Google Authenticator "is a software token that implements two-step verification services using the Time-based One-time Password Algorithm and HMAC-based One-time Password Algorithm, for authenticating users…"[xii]. This means that codes generated by the app are wiped and refreshed every few seconds, cannot be used multiple times, and are not transmitted to the user by being displayed only in the app itself. This makes them difficult to trace or use by a third party, and provides durable multi-factor authentication for AWS.

2. Cloud Platform Security

As you've likely already guessed, AWS is the cloud platform of choice at Brick Bridge. There's a variety of reasons why it is so useful for the projects we do, and security remains one of its strong points. It just so happens that Podio also uses AWS for the backbone of its data storage and security. With AWS having an estimated "42% of the Cloud market by revenue"[xiii] and the AWS S3 service powering 150,000+ websites, it is the premiere choice for much of the internet for operational efficiency. By comparison, Microsoft and Google trail far behind (see Figure 1 below[xiv]) A great portion of the internet relies on Amazon, and as such, it must have rigorous security standards.

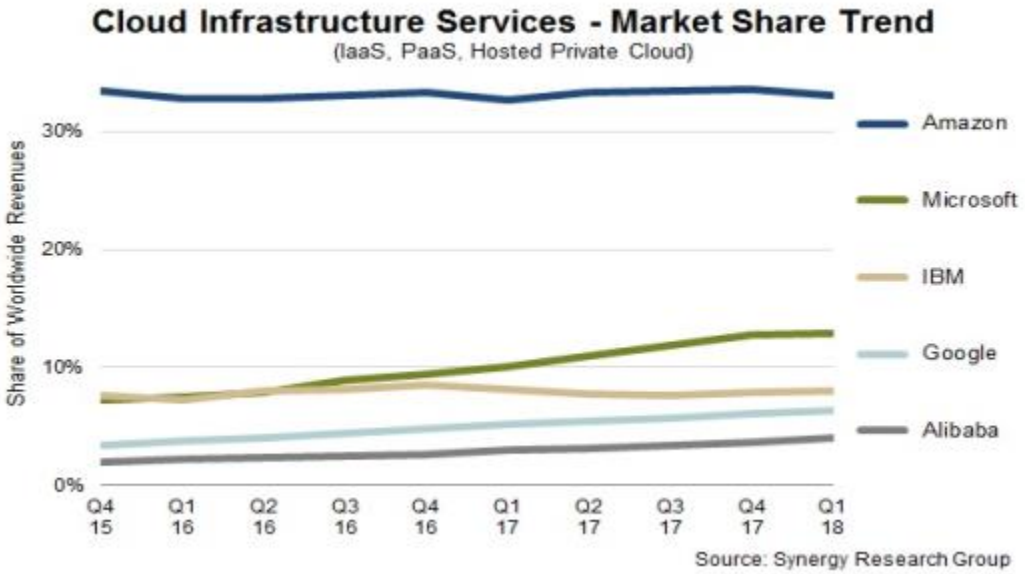

Figure 1- Amazon Continues to dominate the Cloud Computing market in 2018.

AWS employs a number of security platform features to keep consumer data safe, increase privacy, and even secure network access. Amazon has built several technologies such as autoscaling, CloudFront, and Route 53 to help mitigate DDoS attacks on data centers by automatically responding to these events to lessen impact. There are a variety of encryption services available, giving administrators vast control over how data is encrypted. Admins can

even choose whether Amazon automatically manages encryption keys versus managing them manually. Amazon Inspector automatically assesses applications to pinpoint vulnerabilities and deviations from best practice. These services, along with countless others, are backed by a global infrastructure with locations throughout the U.S., Canada, China, South America, Europe, and Asia Pacific. All centers maintain consistent levels of service and security compliance, even going so far as to replicate applications in multiple data centers so they do not experience downtime in case one center goes down. With all these features, it must've been an easy choice for Podio, as well as the development team at Brick Bridge.

As for the reliability of the AWS platform, according to Wikipedia, there are only five major outages since its launch in 2006[xv]. Of these, the last documented outage occurred Feb 28, 2017. and only one of them seemed to have affected multiple global regions, with the rest being localized to an outage at a single region. Three of these incidents occurred due to weather-induced or mechanical power outages, one from an internal memory leak bug, and the most recent occurred from an employee's mistake. It is important to note that none of the above documented outages were caused by deliberate external attacks. It is easy to assume that Amazon would be a big target for attackers, but according to this 2017 article[xvi] and many articles like it, successful attacks manage to exploit end users who have, in most cases, configured their applications inappropriately and have left vulnerabilities intact, which is more of a fault of the end-user and not a fault of Amazon. In these cases, Amazon Services as a whole are not affected. There are numerous instances of companies dealing with AWS data breaches, even large companies such as Tesla[xvii] and Uber[xviii] in recent years, which in the case of Uber, ultimately affected "millions of Uber users" by exposing their personal data.

3. Physical Security at Brick Bridge Consulting

Being a start-up situated in a small office, physical security is not seen as a top priority at Brick Bridge. The office is a suite in an office complex, and as such in addition to all employees having keys for the office and the building's front door, keys for the building are also held by the landlord, the property manager, and any maintenance staff that are associated with the complex. Despite the office complex being quite large, with at least a dozen buildings, and numerous businesses within, there are no dedicated security staff present onsite. It is ultimately up to the tenant to maintain their own security. For Brick Bridge Consulting, this relatively simple system. There is simply an extra deadbolt on the office door, which only employees have a key to. There is also a security camera in the office that stores recordings on the Cloud. The camera has the added benefit of alerting Gil via a mobile notification if it detects activity in the office after designated hours or on the weekend, so he can respond quickly if necessary.

As for hardware security, all employees utilize their personal laptops to conduct their work, and are responsible for keeping up with them. All employees take their computers home with them at the end of the day and there are no dedicated workstations onsite. This creates a point of liability, as if one employee's computer were to be stolen, the thief could then potentially damage any project or any sensitive information that the given employee had been working on. On the same note, having dedicated workstations onsite create the same risk, but that risk could be mitigated by having the appropriate physical security in place.

Conclusion and Security Recommendations

Brick Bridge Consulting, through a combination of platform practice and policy, has built a security model that works for their business. This isn't to say that the model is flawless, but care is consistently taken to ensure that risk can be reduced to a level that is realistic given the scale of the business itself. By utilizing Cloud-based platforms and technologies, clients can have the expectations and peace of mind that their data is secure in the hands of companies that are willing to put their reputations at stake by absorbing the responsibility for the data, and whose business relies on having large numbers of trusted customers. At its current scale, I would argue that Brick Bridge Consulting is effectively managing their security and protecting their assets. With that being said, the company is expanding in both client base and company size, so going forward, more care should likely be taken in order for those assets to remain fully secure.

The most basic recommendation one could make is for Brick Bridge to implement more physical security. While very little asset value is held onsite, the simple installation of an alarm system could deter petty thieves from attempting a break-in and damaging non-essential company property.

Employees have also made a bad habit of sharing code snippets and other potentially sensitive information over the company's group chat in GroupMe. More care should be taken to ensure that sensitive data such as passwords aren't shared electronically.

Lastly, as previously mentioned, employee access should be more carefully limited to projects that they are actively working on in Podio. This could help mitigate intentional tampering or other malicious acts that could occur as a result of an employee having access to a client's live environment. This would damage not only the client, but the business relationship

between Brick Bridge and the client and could potentially limit future Brick Bridge business endeavors. As employees are the largest threat to information security, the greatest care must be taken to ensure that they are properly trained, policies are enforced, and have access only to the resources they need.

Brick Bridge Consulting has quickly begun to make an impact in Louisville and will hopefully continue to expand into bigger and better things for years to come, with a positive financial and business outlook and connections/clients to influencers throughout metro Louisville and beyond. So far it has been a pleasure working with Brick Bridge and I wish only the best as we continue to grow and develop together.

References and Citations

[i] Brick Bridge Consulting website "Discover a New Method of Funding." Brick Bridge Consulting, www.brickbridgeconsulting.com/

[ii] "Project Management and Collaboration Software." Podio, www.podio.com/

[iii] "Boost Productivity and Save Man Hours by Automating Pretty Much Anything You Can Think of in Your Podio Account." GlobiFlow for Podio - Now Part of Citrix, www.globiflow.com/

[iv] "Amazon Web Services (AWS) - Cloud Computing Services." Amazon, Amazon, www.aws.amazon.com/

[v] Greenberg, Andy. "The CCleaner Malware Fiasco Targeted at Least 18 Specific Tech Firms." Wired, Conde Nast, 25 Sept. 2017, www.wired.com/story/ccleaner-malware-targeted-tech-firms/

[vi] Podio Security Specifications https://podio.com/

[vii] "ISO/IEC 27000 Family - Information Security Management Systems." 97.170 - Body Care Equipment, 29 Aug. 2017, www.iso.org/isoiec-27001-information-security.html

[viii] White Paper https://dgyqr055mfays.cloudfront.net/site/resources/podio_security_white_paper.pdf

[ix] Atlassian. "Jira | Issue & Project Tracking Software." Atlassian, Atlassian, www.atlassian.com/software/jira.

[x] Atlassian. "Bitbucket | The Git Solution for Professional Teams." Xerial / Sqlite-Jdbc - Bitbucket, www.bitbucket.org/

[xi] "Hosting Your NuGet, Npm, Bower, Maven, PHP Composer and Vsix Packages." MyGet, MyGet (TechTomato BVBA), www.myget.org/

[xii] "Google Authenticator." Wikipedia, Wikimedia Foundation, 29 June 2018, www.en.wikipedia.org/wiki/Google_Authenticato

[xiii] Weise, Elizabeth. "Does Amazon Control the Internet, or Does It Just Feel That Way?" USA Today, Gannett Satellite Information Network, 1 Mar. 2017, www.usatoday.com/story/tech/talkingtech/2017/03/01/amazon-control-internet-aws-cloud-services-outage/98548762/

[xiv] Figure 1 – Novet, Jordan. "Microsoft Narrows Amazon's Lead in Cloud, but the Gap Remains Large." CNBC, CNBC, 27 Apr. 2018, www.cnbc.com/2018/04/27/microsoft-gains-cloud-market-share-in-q1-but-aws-still-dominates.html.

[xv] "Timeline of Amazon Web Services." Wikipedia, Wikimedia Foundation, 24 June 2018, www.en.wikipedia.org/wiki/Timeline_of_Amazon_Web_Services

[xvi] Hleb, Nadia. "The Amazon Cloud Has Not Been Hacked but Two Companies Have Been Affected." Softonic, Http://En.softonic.com/, 25 Oct. 2017, www.en.softonic.com/articles/amazon-cloud-has-been-hacked-two-companies-have-been-affected

[xvii] "Tesla Hackers Hijacked Amazon Cloud Account to Mine Cryptocurrency." Fortune, Fortune, www.fortune.com/2018/02/20/tesla-hack-amazon-cloud-cryptocurrency-mining/

[xviii] Rama11/21/2017, Gladys. "Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users." AWSInsider, www.awsinsider.net/articles/2017/11/21/uber-aws-data-breach.aspx