Microsoft Acquisition Risk Analysis

# Abraham Cain

# July 18, 2021

Table of Contents

[Introduction 3](#_Toc77803076)

[Overview 3](#_Toc77803077)

[Microsoft E-Commerce Operations Overview 3](#_Toc77803078)

[Microsoft’s Cybersecurity Needs 4](#_Toc77803079)

[Analysis 5](#_Toc77803080)

[Cybersecurity Industry & Supplier Overview 5](#_Toc77803081)

[Operational Risks Overview 8](#_Toc77803082)

[Product Liability 9](#_Toc77803083)

[Summary and Conclusions 9](#_Toc77803084)

[References 11](#_Toc77803085)

# Introduction

## Overview

Microsoft was founded in 1975 by Paul Allen and Bill Gates in Albuquerque, New Mexico selling software for the Altair 8800 personal computer (history.com Editors, 2020). Though they started out as a computer software company, they have since branched out to several more technology related sectors. Below is a timeline of some of the major events for Microsoft using information found on Microsoft’s website (2021) and Brittanica (Pascal and Hall, 2021) :  
1975 – Founded  
1981 – Incorporated  
1981 – Gets IBM to produce personal computers with MS-DOS 1.0 Operating System  
1989 – Launches Microsoft Office software  
1995 – Launches Windows 95 which was their first integration of MS-DOS with Windows GUI  
2001 – Releases XBOX game console getting into the video game market  
2010 – Releases Windows Phone 7 their first phone  
2010 – Launches Windows Azure getting into the cloud market

2016 – Acquires LinkedIn entering the social media market

2019 – Releases Hololens 2 Mixed Reality device

## Microsoft E-Commerce Operations Overview

According to their Hoover report (Hoover, 2021), Microsoft’s operations are split into three different sections: “More Personal Computing, Productivity and Business Processes, and Intelligent Cloud” (p. 3, core report). They go on to show the breakdown of revenue by operational department as follows:

More Personal Computing – 35%

Productivity and Business Processes – about 33%

Intelligent Cloud – about 30%

Within the more personal computing operational department falls products and services such as Xbox, Windows Operating Systems, Surface Pro Tablets, HoloLens VR headsets, phones, royalties on games, and the like. Productivity and business processes consists of their software suites such as Office365, Dynamics ERP and CRM, and Skype products. Azure as well as anything cloud computing related falls under the third category. They currently have over 175,508 employees worldwide, 101,277 in the US, and almost 50% of them are engineers of a sort (Microsoft, 2021). According to their 10-K report (Brod, 2019)

## Microsoft’s Cybersecurity Needs

Microsoft being a large company has a broader range of assets that need protecting from cybersecurity threats. I will break down threats and cybersecurity needs based on the three previously identified operational functions: Personal Computing, Productivity/Business Process Software, and Intelligent Cloud.

In the personal computing arena, Microsoft must consider the security of the operating systems and devices that they release to their customers. When there are vulnerabilities found in their products, they must have a team ready to fix the issues and push updates out to customers (Norton, 2021). They also must have teams of researchers actively looking for vulnerabilities and staying on top of the latest malware so that they can keep up-to-date “virus signatures” for their Windows Defender products which come installed in Windows 10 systems. Besides protecting their customers, Microsoft also must employ an information security management system organization-wide to address risk and cybersecurity issues. They must control access to proprietary information such as product research and development, operating system source code, and any business processes or information that could be targeted by hackers or insider threats for personal gain/industrial espionage.

Microsoft’s productivity and business software must be kept safe as well. Customers rely on their exchange servers to keep emails confidential and ensure proper encryption and non-repudiation are available for consumers. This is especially evident with the recent vulnerabilities being exploited in Microsoft Exchange servers allowing threat actors to gain access to organizations and snoop on emails of victim organizations (Osborne, 2021). These productivity software applications can be used as an entry point into the networks to steal information, deploy ransomware, or even destroy data.

Microsoft’s security requirements and needs expand to their intelligent cloud services as well. They must also restrict physical access to buildings to stay compliant with PCI DSS (Tunggal, 2021) and NIST CSF DE.CM-2 since they have federal cloud contracts (Reciprocity, 2021)(US DoD, 2019)(CSF Tools, 2018). They are also responsible for ensuring the confidentiality of their customer’s data in the cloud and defending against side channel attacks, VM escape attacks, and denial of service attacks to name a few (Bryk, 2020). Microsoft may also have to be on the lookout for criminals and terrorists utilizing resources from Azure to carry out denial of service attacks or hosting malicious/inappropriate content.

# Analysis

## Cybersecurity Industry & Supplier Overview

Cybersecurity like so many other things in life has become monetized. Cybersecurity as a market exists because somebody realized that they could sell products and services to make systems more secure. The reason that people and companies are willing to spend money to purchase, learn about, and implement these products and services is because people started losing money, reputation, and data they deemed sensitive to cyber criminals and eventually nation state cyber adversaries as well. It is therefore in the best interest of companies and sometimes even everyday users of computers to utilize security tools and products to prevent such things from happening.

Cybersecurity is less about guarding electronic devices and more about safeguarding the confidentiality, availability and integrity of data and communications. It is about guarding people’s reputations, wallets, and keeping the lights on and the gasoline flowing. Computers were originally invented to make life easier and allow us to solve problems faster and more efficiently. This holds true today as cloud computing, personal computers, and software applications streamline communication, mathematical processing, and are integrated into many aspects of modern civilization. I liken cybersecurity’s role in modern day computing to security features in cars. People manufacture cars with airbags to decrease the chances of death or injury to passengers in accidents. By far, the most effective security measure for avoiding injury or death of passengers would be to manufacture a car that is immobile or that does not move. However, a car that is incapable of transport is pointless. In the same way, there is a balance to be played with cybersecurity products and services. They must enable businesses to be productive while maintaining safety. A computer incapable of calculations or accessing necessary data is pointless.

Microsoft has need for cybersecurity products that may be integrated with their products or used to improve their own products. As previously mentioned, Microsoft’s personal computing products have need to be secured against the continuous barrage of vulnerabilities and exploits developed by persons and groups with ill intention. In answer to this need, they would benefit from taking in threat intelligence feeds and crowdsourced bug-hunting programs. Bugcrowd is an organization that offers crowdsourced bug hunting to e-commerce and software providers. Vulnerability researchers, known as bug hunters, sign up with Bugcrowd to search for vulnerabilities in customer’s products and infrastructures at the discretion of the customer in return for rewards in the form of payment, reputation points, or company-themed merchandise (Bugcrowd, 2021).

In addition to crowdsourced bug-hunting and responsible disclosure programs, Microsoft needs a continuous feed of cutting-edge intelligence. They need to know of trends in the threat landscape before they become public or popular. This creates need for a threat intelligence service. The renowned Mandiant FireEye provides their product Mandiant Advantage, a cutting-edge threat intelligence platform that utilizes data from current incidents, research, and dark web forums (Mandiant, 2021).

One of the more tangible areas of cybersecurity is physical security. Microsoft’s cloud environment requires physical security at the physical datacenters and R&D labs. All data stored or processed in the cloud is stored or processed on a physical machine. If the physical machine is accessed or damaged in-person, no amount of network or host-based controls can stop the incident. As we discussed earlier, Microsoft has locations across the globe. To provide physical security of facilities, they could benefit from the security guarding services of international physical security specialists: Securitas. According to their website, Securitas provides services in North America, Europe, Ibero-America and AMEA which stands for Africa, Middle East, Asia, Australia (Securitas, 2021).

## Operational Risks Overview

One only needs to turn on the news to see how suppliers of cybersecurity or IT tools and services may be sources of risk for a company using their services. In 2020, it was disclosed that SolarWinds Orion software had been compromised and used to gain access to networks of over 18,000 customers (Hope, 2020) (FireEye, 2020). It is important to recognize risks associated with our vendors and suppliers.

Bugcrowd has risk in the area that Microsoft may not know who is probing their systems or code for vulnerabilities. It is also possible that by welcoming systems to bug testing, Microsoft may open themselves up to unintentional damage from a less-skilled bug-hunter who uses automated tools for hacking and leaves behind a backdoor or accidentally causes a Denial of Service (DoS) attack. The biggest area of concern for Bugcrowd would be insider threats and Microsoft not knowing the backgrounds of the people attempting to disrupt or break into their systems and their level of training.

The only big risk that comes from utilizing threat intelligence services from Mandiant Advantage and other threat intel providers comes from what information you allow them to have access to. If you participate in sharing internal threat intelligence with FireEye, you run the risk of that intelligence going public if FireEye is hacked or the data is leaked by an insider at FireEye. This could expose internal operating procedures, network architecture, technologies, and/or sensitive information if this data is shared with a third party.

Securitas is perhaps the hardest to defend against in risk management. Since the very nature of their physical security services are to have a third-party guard your most precious physical resources such as datacenters, research labs, or even records archives, the risk of a malicious or negligent insider poses a great risk to physical security. Unless Microsoft can establish a vetting process for guards hired to secure access to facilities and resources, there is no way of knowing for sure that the guards could not be bribed to look the other way for criminals. A security guard could be selling badges to enter buildings or accepting bribes to abandon their post so that criminals gain access to restricted areas.

## Product Liability

According to Attorney at Law, Kathy Winger (N.D.), businesses may be liable for data breaches of vendors with whom you share confidential information. It does however depend on your contracts with them. Therefore, it is crucial that Microsoft, among other reasons, maintain an exceptional legal team. They should look over contracts carefully and make adjustments before coming to an agreement with vendors, as necessary.

# Summary and Conclusions

In summary, it is important that Microsoft consider the risks and rewards for adopting products and services from vendors. There are almost always risks associated with adopting a new tool and one must ask themselves if they can trust the vendor to secure any data shared with them. To address these risks, one could transfer the risk, accept the risk, mitigate the risk, or avoid the risk. By avoiding risk, Microsoft would reject the product or vendor. To mitigate the risk, Microsoft could accept the product or vendor and put into place compensating controls to decrease the likelihood of an undesirable outcome. By accepting the risk, they would be deciding that the risk is not high enough to warrant concern or action and then they would accept the product without further controls. By transferring risk, Microsoft could through legal and/or contractual means, have the vendor take responsibility for risks in a legally binding agreement. Whatever they do, Microsoft must be aware of the risks associated with third-party trust and place thought into their acquisitions and contract renewals.

# References

Brod, F. H. (2019). Form 10-K 2019. <https://www.sec.gov/Archives/edgar/data/789019/000156459019027952/msft-10k_20190630.htm>

Bryk, A. (2020, February 26). Cloud computing attacks: A new vector for cyber attacks. Apriorit. <https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks>

Bugcrowd. (2019, March 27). Bug bounty program list - All active programs in 2021 | Bugcrowd. Retrieved July 19, 2021, from <https://www.bugcrowd.com/bug-bounty-list/>CSF Tools. (2021, May 29). CSF version 1.1. <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/>

D&B Hoovers. (2021). Onestop Report Microsoft Corporation. <https://app-avention-com.ezproxy.umgc.edu/company/beb446af-bfe3-3775-a1f4-491c4fae4e9b>  
This URL may require you to log into an account to access the report

FireEye. (2020, December 13). Highly evasive attacker leverages SolarWinds supply chain to compromise multiple global victims with sunburst Backdoor. Retrieved July 20, 2021, from <https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html>

Hall, M. and Zachary, . Gregg Pascal (2020, November 12). Microsoft Corporation. Encyclopedia Britannica. https://www.britannica.com/topic/Microsoft-Corporation

History.com Editors. (2015, October 9). Microsoft founded. HISTORY. <https://www.history.com/this-day-in-history/microsoft-founded>

Hope, A. (2020, December 24). Solarwinds Backdoor affected 18,000 customers; Microsoft warns 40 actively targeted organizations. CPO Magazine. <https://www.cpomagazine.com/cyber-security/solarwinds-backdoor-affected-18000-customers-microsoft-warns-40-actively-targeted-organizations/>

Ironscales. (2021). Our story. <https://ironscales.com/our-story/>

Mandiant. (2021). Cyber threat intelligence. FireEye. Retrieved July 19, 2021, from <https://www.fireeye.com/mandiant/threat-intelligence.html>

Osborne, C. (2021, March 16). Everything you need to know about the Microsoft exchange server hack. ZDNet. <https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/>

Reciprocity Labs. (n.d.). Is NIST mandatory? <https://reciprocitylabs.com/resources/is-nist-mandatory/#:~:text=NIST%20compliance%20is%20mandatory%20for%20federal%20agencies%20and,federal%20agencies%2C%20and%20has%20been%20so%20since%202017>

Securitas. (2020). Our organization. Retrieved July 20, 2021, from <https://www.securitas.com/en/about-us/our-organization/>

Symanovich, S. (2021, January 23). 5 reasons why general software updates and patches are important. NortonLifeLock. <https://us.norton.com/internetsecurity-how-to-the-importance-of-general-software-updates-and-patches.html>

Tunggal, A. T. (2021, May 25). What is access control? The essential cybersecurity practice. UpGuard. <https://www.upguard.com/blog/access-control>

U.S. DEPARTMENT OF DEFENSE. (2019, October 25). Contracts for October 25, 2019. Retrieved July 5, 2021, from <https://www.defense.gov/Newsroom/Contracts/Contract/Article/1999639/>

Winger, K. (n.d.). Cybersecurity and data breaches from a business lawyer’s perspective [Introduction]. GSX. <https://www.gsx.org/gsx-blog/can-you-be-liable-for-your-vendors-data-breach/>