## VTech as a Case Study: Importance of Investment in Cyber Security

Cyber threats are growing starkly on a global scale. There has been a tremendous increase in mobile malware attacks from 2017 to 2018 alone. The number has nearly doubled – from 66.4 million to 116.5 million attacks (Kaspersky, 2019). Furthermore, there have been significant breaches in that year as well. Global businesses, such as Facebook, Marriott and Quora have been hacked with millions of users being affected (Malwarebytes, 2019).

One would think that companies would invest more money with the steady increase in threat. On the contrary, the mean spending on cyber security for UK businesses in 2019 only amounted to £5,100 with median spending of £200. This demonstrates, that while there might be a few more prominent companies spending larger amounts on their security investments, there are a lot more companies spending little to nothing. Additionally, out of the 1,566 UK businesses that were surveyed, 33% have spent nothing on cyber security at all (Department for Digital, Culture, Media and Sport, 2019).

This already presents a massive risk for companies on the current date. One such example is the company VTech. VTech is the largest manufacturer and supplier for electronic learning products with products mostly marketed towards infants, toddlers and preschoolers (VTech, N.D.). In 2015, the company experienced a hack that exposed a multitude of data, including names, postal addresses, email addresses, IPs and even pictures and audio logs of their young customer base and their parents. In total, VTech confirmed that about five million customer accounts and children's profiles had been compromised with the customers mainly being from the US, Europe and Canada (Eadicicco, 2015). This resulted in substantial financial damages for the company. "Vtech's stock has fallen 22 percent this year, giving the company a market value of HK$21.9 billion ($2.8 billion)" (Reuters, 2015). Following the hack, the shares of VTech Holdings Ltd and other VTech securities were suspended from trade (Reuters, 2015).

Alarmingly, it was reported that VTech knew about pre-existing security flaws for more than two years prior to the hack (Brewster, 2015). The hack itself was conducted via an SQL injection: a widespread attack vector, that was already on top of the list of most critical web application security risks in 2013 (OWASP, 2013). VTech should have accounted for this vulnerability. Following the hack, VTech, a company that recorded revenues of $1.9 billion in 2015, refused to answer whether they even had a security team in place (Brewster, 2015).

This is one of the many case studies wherein companies have been hacked due to a lack of investment and awareness of cyber security threats. This highlights the importance of cyber security and how a focus on this can save companies millions in reputational and financial damage.

## Reference List


Brewster, T. (2015) More Trouble For VTech -- Kids Tablet Is 'Easy' To Hack. Forbes. Available from: https://www.forbes.com/sites/thomasbrewster/2015/12/02/vtech-innotab-tablet-easy-to-steal-kids-data/#5f66ade32863 [Accessed 26 September 2020].

Department for Digital, Culture, Media and Sport (2019) Cyber Security Breachers Survey 2019. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf [Accessed 26 September 2020].

Eadicicco, L. (2015) Everything to Know About a Massive Hack Targeting Children's Toys. Time. Available from: https://time.com/4130704/vtech-hack-childrens-toys/ [Accessed 26 September 2020].

Kaspersky (2019) The number of mobile malware attacks doubles in 2018, as cybercriminals sharpen their distribution strategies. Available from: https://www.kaspersky.com/about/press-releases/2019_the-number-of-mobile-malware-attacks-doubles-in-2018-as-cybercriminals-sharpen-their-distribution-strategies [Accessed 26 September 2020].

Malwarebytes (2019) 2019 State of Malware. Available from: https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf [Accessed 26 September 2020].

OWASP (2013) OWASP Top 10 - 2013. Available from: https://owasp.org/www-pdf-archive/OWASP_Top_10_-_2013.pdf [Accessed 26 September 2020].

Reuters (2015) Shares in Hong Kong toy maker VTech halted after customer data stolen. Available from: https://www.reuters.com/article/vtech-cyberattack/shares-in-hong-kong-toy-maker-vtech-halted-after-customer-data-stolen-idUSL3N13P0LY20151130 [Accessed 26 September 2020]

VTech (N.D.) About Us. Available from: https://www.vtech.com/en/about-us/ [Accessed 26 September 2020].

## Post-Discussion Summary: VTech as a Case Study

Using VTech as a case study, it was highlighted that the lack of investment and awareness in cyber security by the company's top management is one of the main obstacles cyber security professionals face. I agree that this is a fundamental issue that needs be addressed in most organisations. Most of the time, the top non-technical management view the operations from a pure business standpoint, taking mostly profit and loss impacts into account. There is an apparent disconnect between key decision-makers and the technical understanding of putting such measures in place. Therefore, it is vital that a security professional can persuade management to prioritise investments in security as a preventive measure.

First and foremost, the management needs to be informed about all potential implications should a breach occur. This needs to be conveyed in a comprehensive language that every stakeholder understands. Furthermore, it is vital to highlight the actual impact on potential profits and losses should measures be put in place, such as prevention of monetary losses or future cost benefits.

A second point that may help to persuade upper management is to understand the business context of the company or organisation. "The business context encompasses an understanding of the factors impacting the business from various perspectives, including how decisions are made and what the business is ultimately trying to achieve" (business wire, 2018). By knowing what is essential to the organisation, one can ensure that proposed initiatives are aligned to the needs of key business decision-makers.

Lastly, one can consider local laws to drive the argumentation. By being aware of the legislation, a security professional can inform management about regulatory requirements and potential fines, should a company not comply.

In conclusion, whilst cyber security measures do not necessarily always prevent a breach, it still is essential to inform management about consequences of such incidents and the impact they can have on the organisation. Stakeholders can then come to an informed decision about the necessary resources to allocate for security measures.

## Reference List

Business Wire (2018) Define the Business Context Needed to Complete Strategic IT Initiatives: 2018 Blueprint. Available from: https://www.businesswire.com/news/home/20180201006534/en/Define-the-Business-Context-Needed-to-Complete-Strategic-IT-Initiatives-2018-Blueprint---ResearchAndMarkets.com [Accessed 11 October 2020].