Discussion Forum-1 Peer Response:

Post by **Sahib Jabbal**

144 days ago

Peer Response

Hi Gokul,
Very insightful post regarding e-commerce and cybersecurity.

I concur with you that e-commerce has become a major revolution over the years and keeps growing. With the revolution of e-commerce and wide use of e-commerce platforms such as Amazon, eBay, and well-known brands incorporating e-commerce platforms to generate sales, these sites shall remain a target for cyber-attacks. (Ecommerce Security: Securing Against Cyber Threats 2022 | BigCommerce | BigCommerce, 2022).

With sensitive personal data and other data stored on these e-commerce platforms, individuals should be aware of what information is shared on these platforms such as payment details and payment gateways are acceptable by the e-commerce platforms such as PayPal, VISA, Mastercard, Apple Pay in specific regions and mobile money such as M-Pesa (commonly used in Kenya).

Business owners have been aware of the security concerns on e-commerce platforms and according to the VMWare Carbon Black 2020 Cybersecurity Outlook report, it was found that about 77% of businesses surveyed had purchased new security products between 2019 and 2020. In addition, about 69% had increased security personnel. (Ecommerce Security: Securing Against Cyber Threats 2022 | BigCommerce | BigCommerce, 2022).

References:

BigCommerce. 2022. *Ecommerce Security: Securing Against Cyber Threats 2022 | BigCommerce | BigCommerce*. [online] Available at: [Accessed 17 March 2022].

209 words

Post by **Abraham Gordon**

144 days ago

Peer Response

Hello Gokul,

Thank you for this insight; I most certainly agree that the E-Commerce industry has had profound changes that impact the average user immensely.

Your arguments have a theme of being linked to financial gain(s), and to further support your statements, UK finance reported that in 2010, greater than 50% of payments within the United Kingdom were made via cash in comparison to just 17% of payments now being made via cash in 2020 (Buckle, 2021). The increase in digital payments results in a more significant requirement for cyber security assurance activities such as audits, penetration testing and table-top exercises to ensure sufficient cyber-resilience for digital transactions.

You detailed that “*the key reasons an organisation should invest in cyber security are to maximise profit, retain customers and the company, and mitigate the hazards connected with remote working.*” Could you further expand upon the remote working “hazards”? Why is this now a greater risk to companies? Does remote working even present a greater risk if networks are secure by design? Enterprise architects should be aiming to implement future-proofed, optimised solutions, thus minimising the impact during significant changes such as those observed during the COVID-19 pandemic. If systems or networks are secure and optimised by design, inclusive of processes, guides and standards, the only residual risks should be that of zero-day vulnerabilities and obsolescence.

References:

Buckle, A. (2021) impact-covid-19-cash. Available from: **https://www.ukfinance.org.uk/news-and-insight/blogs/impact-covid-19-cash** [Accessed 17/03/2022].

236 words

Reply

Rate: 1 ?? ▾

1 reply

1.

Reply to **Abraham Gordon** from **Gokul Kurunthasalam****Parent of this post↑**

134 days ago

Reply post for Peer Response

Thank you for your valuable feedback. To answer your questions, work from home or remote logging is a significant challenge for a variety of reasons. For an example, ignoring Common Sense Physical Security in Public Places. Even though cybersecurity is our primary objective, we cannot ignore physical security when it comes to company's important information. For instance, some employees may converse loudly on the phone while working in public areas, display their laptop's screen to the entire crowd inside a café, or even leave their equipment unattended.

In the United Kingdom alone, 66% of surveyed organizations reported a successful phishing attempt and 30% reported malware infection as a result. According to a recent poll conducted by Tessian, a security business based in the United Kingdom and the United States, 56 percent of senior IT professionals believe their staff have developed undesirable cyber-security behaviors while working from home. Worryingly, the study discovered that a sizable number of employees concurred with such judgement. We are having uncontrollable things when we do remote logging, which is a greater risk for companies.

Businesses should educate their staff on even the most fundamental security procedures, even if they appear to be self-evident. Businesses should invest in providing effective and efficient training to their employees to ensure they are following proper procedures. Should make available safe devices and a robust VPN connection to ensure adequate security.

References:

"Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy" by Jason R. C. Nurse, Nikki Williams, Emily Collins, Niki Panteli, John Blythe & Ben Koppelman; Conference paper; 03 July 2021