**O’Reilly Design Cybersecurity Analysis**

**Corey Crooks**

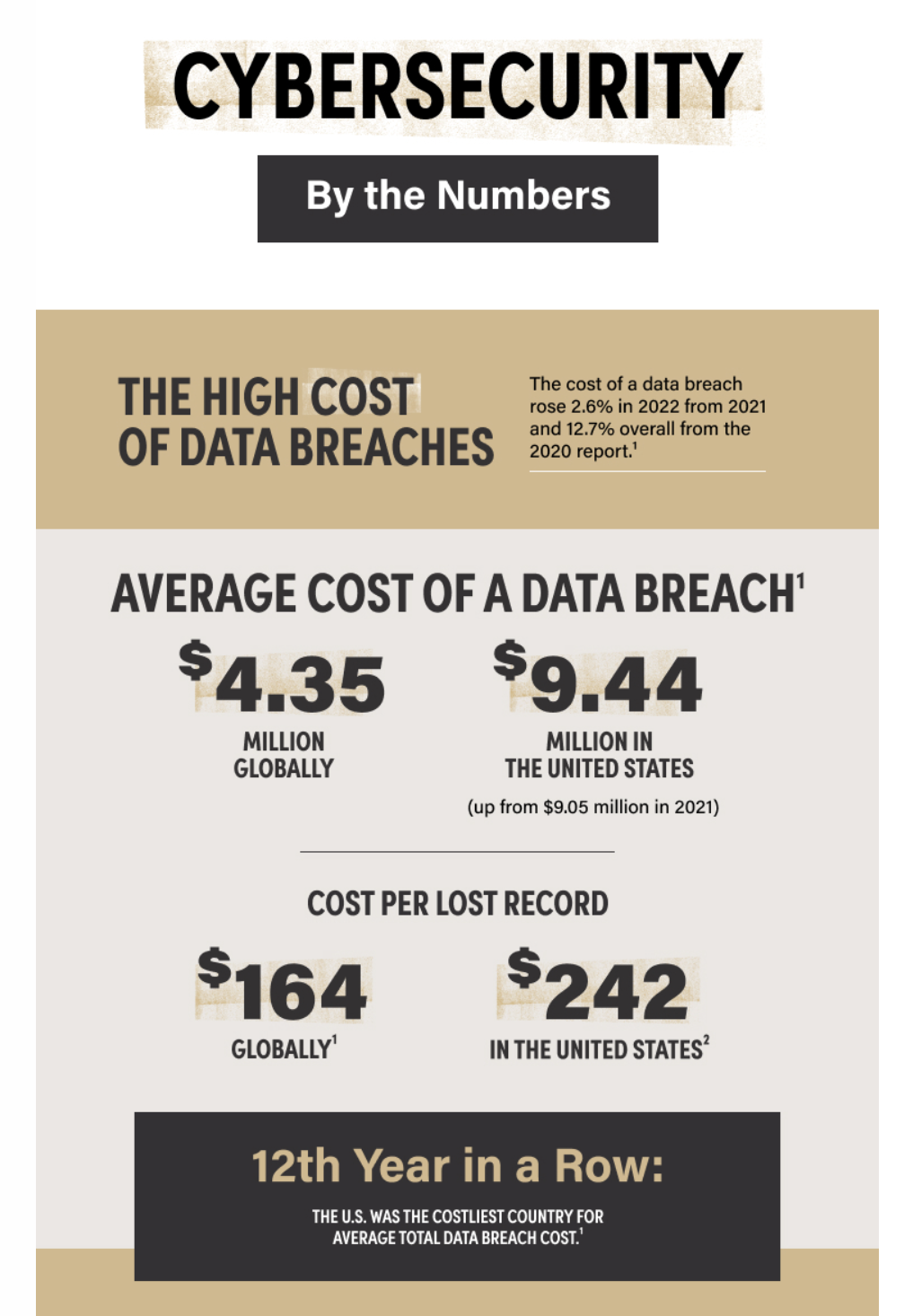
**Purdue University Global**

**IT402—IT Consulting Skills**

**Tom Olmstead**

**November 8th, 2023**

No matter the location, cybercrime is a very real threat. Countless cases happen day by day to vulnerable businesses that cannot protect or recover from an attack. Unfortunately, preventative measures are all too rare. Although it may be cheap to forego the expenditures of preparation, the risk of a cyber attack is far more costly.



(Purdue Global University, n.d.)

The preceding is a graphic from Purdue Global University displaying an average breakdown of risk expenditures relating to cybersecurity breaches. These breaches can come in a number of ways but commonly it can originate from Social Engineering, or a subsect practice of it such as phishing (Clayton State University, n.d.). Social engineering uses the social aspect of a computer system to gain access where a user is not permitted. These can be attempts at convincing employees to open doors, lies to lift security restrictions, or any other inventive way an attacker may use the employees of a site to help them through. One such method is called Phishing. This method sees an email sent to employees of the target. This could entail the attacker posing as a reputable brand looking for either information, or action. For example, the local police in Singapore issued a public statement regarding a phishing attack there. Users of WhatsApp under attack would be sent a QR code, and told to scan it to secure their account (Knight, 2023). In actuality, it was relaying the user’s information to a third party that collects the account information such as passwords and emails of the accounts that scan the QR code. WhatsApp users may be just trying to protect the account they use for vital processes throughout their daily life, but have easily given malicious actors access to that very same account in the process.

There are many ways a business can help secure their operations to a potential attack. Although O’Reilly may never be completely safe from attacks, there are a number of great starting points. First and foremost, I would recommend a complete implementation of employee education regarding the dangers of cybercriminals. As most phishing relies on employee heuristics, they will be the most important bastion of defense to fortify (Solms, n.d.). Educating your employees about common cybersecurity threats would be a wonderful way to ensure that your business may be that much less likely to fall victim to a cybersecurity attack. After all, if your employees know how to spot a cybercriminal at work, they may be able to avoid a situation that has them inadvertently giving precious company data to a malicious actor. It is important that this education goes over common tricks that phishing scams may employ, but it is equally vital that it teaches the employees to be much more aware about their own actions. It is impossible to go over every single phishing scam in existence, and what to look for. For that reason, the employees will need to know how to be cautious of these attempts, even if there are no explicit signs that work talked about in the actual meeting. These scams evolve, or die; so new methodologies are developed daily.

Remember, O’Reilly is not just preventing the lost of data in an event of breach security. Each time a data breach happens, a malicious actor may opt to wipe servers of the company in order to hold the data they gathered for ransom to be paid for the data to be returned. However, there is not just data at risk in this exchange. With each data breach your company undergoes, you risk the goodwill and reputation your clients hold for you as well. Not only your clients, but other malicious actors may also become aware of your company’s weaknesses, and may perpetuate more attacks towards your company in an attempt to capitalize on this “easy prey”. Moreover, employees may lose respect for the company they dedicate their time to, should it seem that management is disregarding their own personal cyber-safety. After all, it is not just client information that is stored on your company servers.

O’Reilly finds itself particularly at risk of phishing scams. Having a decent business is one possible reason for being a target, but the avenues of traffic O’Reilly has opened up to are additional risks that need to be considered. I understand that O’Reilly has a web presence that serves as a point of sales option for customers to utilize for their own convenience. This creates an additional opportunity for malicious actors to capitalize on (Cleveland State University, n.d.). A web presence presents the position of an actor to gather internet traffic from clients trying to connect to the service. If they are able, they may attempt to make a mirror site that tricks customers and clients into believing that they are indeed your storefront. From there, each and every user that enters the site could be at risk of having important and vital information stolen. This could cost precious goodwill from your clients as mentioned previously, and completely collapse potential growth investments.

All these reasons and more outline the numerous dangers the cyber climate presents to O’Reilly. It is imperative that the company is proactive about loss prevention, and cognizant about the countless dangers the company faces every moment they are online. Cybersecurity threats like Phishing are never completely avoidable, but there are plenty of steps that can be taken to both minimize loss in an attacking event, or mitigate the chances a malicious threat has to do damage to the hardworking individuals of O’Reilly.

# **References**

Clayton State University. (n.d.). *Social Engineering*. Retrieved from Information Security: https://www.clayton.edu/its/it-security/cyber/index

Cleveland State University. (n.d.). *More About Phishing*. Retrieved from csuohio.edu: https://www.csuohio.edu/phishing/more-about-phishing

Knight, O. (2023, November 3). *Singapore Police Issue Warning Over WhatsApp Phishing Scam*. Retrieved from CoinDesk: https://www.coindesk.com/business/2023/11/03/singapore-police-issue-warning-over-whatsapp-phishing-scam/

Purdue Global University. (n.d.). *Cybersecurity by the Numbers*. Retrieved from purdueglobal.edu: https://www.purdueglobal.edu/blog/information-technology/cybersecurity-by-the-numbers-infographic/

Solms, E. D. (n.d.). *Phishing: How an Organization can Protect Itself*. Retrieved from Nelson Mandela Metropolitan University, South Africa: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ed02ea2655cc0b303988a1eae273418b37665939