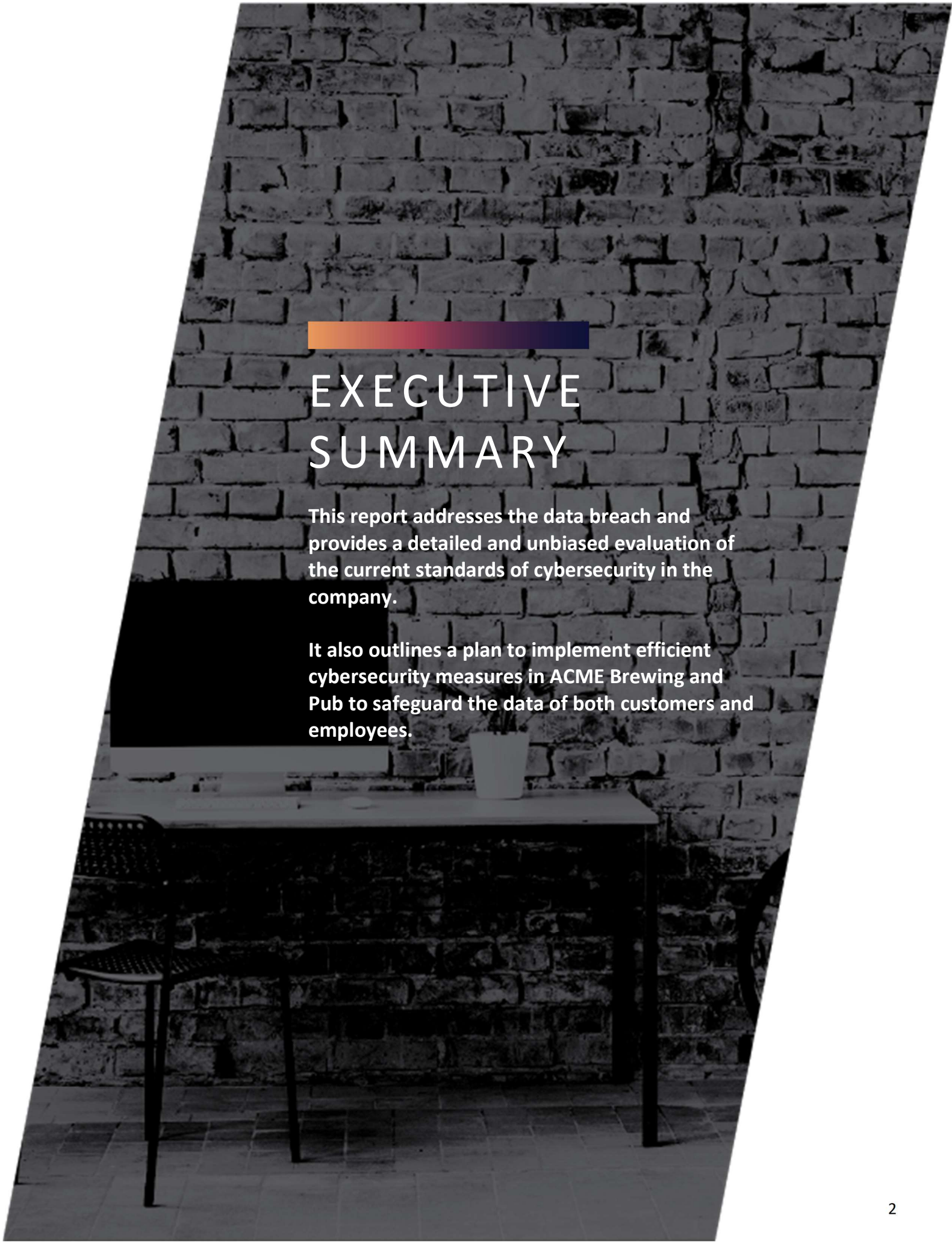
CYBERSECURITY MEASURES

SAFEWEB.INC

LAKSHMI S | LAKSHMIBRAHMANI.SURAVAJJALA@UCDENVER.EDU



EXECUTIVE SUMMARY

This report addresses the data breach and provides a detailed and unbiased evaluation of the current standards of cybersecurity in the company.

It also outlines a plan to implement efficient cybersecurity measures in ACME Brewing and Pub to safeguard the data of both customers and employees.

CYBERSECURITY AWARENESS

In the ever-evolving world of digitalization where more and more people are using online services and companies are rebranding and changing the way they serve customers. So it's the company's added responsibility to protect the customer's data and their privacy.

Digitalization and storage of customers' data have attracted many cyber hackers to steal this information by various means and use them maliciously. So, to avoid these attacks it is very important for the companies to include cyber security practices in their product development cycles and in their culture.

ACME Brewing and Pub could have averted the pitfalls that it had faced if they had given importance to cyber security and understood the effects of poor cyber security on their customers and employee. In addition to strengthening the IT department with cyber security professionals, it should include security in their work culture and change their perspective about cyber-attacks to protect their customers' data.

ACME Brewing and Pub store customer card information and employees' sensitive data. It is more than important for it to follow Payment card industry data security standards (PCI-DSS). PCI-DSS provides requirements and guidelines for the companies to protect the cardholder's information. Companies should adhere to the requirements of PCI-DSS when they are dealing with cardholder data to avoid any penalties in the event of a breach. ACME Brewing and Pub should implement these requirements in every step of their business and product development.

Cyber security is more than technical implementation, it should be imbibed in the culture of the company. Customers' data and their privacy should be equally important as their product. ACME Brewing and Pub requires a cultural shift of their mindsets to implement best practices and industry standards in protecting the data.

PHISHING

Phishing is the practice of tricking people through deceptive emails or messages into revealing personal or confidential information, which can then be used maliciously against the firm or the person. In this case, the personal data of the employees is breached and leaked outside the ACME brewing and pub as a result of a phishing email. This information can be used for identity theft and to impersonate the employee, leading to substantial personal and financial loss to the employees and their families.

Understanding common types of phishing scams

- Clone phishing: Clone phishing is a sort of phishing scam in which the hacker clones a legitimate email message sent by a trustworthy company. The hacker modifies the email by replacing or adding a link that leads to a harmful and fake website.

- Spear phishing: Spear phishing is a type of phishing that targets specific individuals or groups within a company. It is a powerful variant of phishing, a malicious method that leverages emails, social media, instant messaging, and other platforms to trick people into disclosing personal information or performing acts that result in network compromise, data loss, or financial loss.

- Whale phishing: A whaling attack is a type of spear-phishing attack targeted at high-level executives in which attackers pose as legitimate, well-known, and trusted entities and push the victim to share extremely sensitive information or to send a wire transfer to a fraudulent account.

- Tech support phishing: Tech support Phishing emails allege that your device is infected with malware. To "repair" the problem, the hacker will ask to install remote access software on your device but instead installs malware.

ACME Brewing and Pub has faced Whale phishing, where the director of HR was targeted to reveal sensitive information about employees. This has occurred due to the management’s lack of awareness about phishing and techniques to identify these emails. There are no standards and policies in the firm on sharing sensitive information across the personnel.

ACME Brewing and pub should implement the following measures to avoid any potential risk through phishing in the future,

- Frame policies and standards on sharing information both sensitive and non-sensitive within the company.
- Do not provide personal or confidential information unless you have verified it directly with the person making the request.
- Pay close attention to the content of the email and the email addresses of the sender before replying or forwarding it.
- Install security software, spam filters, and firewall programs that are effective in identifying phishing attacks.
- Use multi-factor authentication for accessing sensitive information.
- Educate your personnel and hold training sessions with mock phishing scenarios and emails.
- Encrypt all sensitive company information while storing and sharing it across the company.
- Keep all the devices updated with the latest security patches and strong anti-virus softwares.
- Have regular security checks across the company to identify any vulnerabilities.

WEB AND DATA BACKUPS

Data security is an important aspect of business operations, and data backups are an important part of that strategy. Data backups ensure that you have a complete copy of your systems ready to restore, regardless of the cause of the data loss. Along with the data backups, it is equally important to have a webpage backup.

ACME Brewing and Pub had lost the website due to word press corruption and which in turn lost the business from their customers. This could had been averted if they had a working backup to replace the corrupted website and also had tested any changes in the development environment before deploying it to production.

It is important for the company to understand the benefits of having working web backups. A working backup could protect your website from human error. Because the company's primary focus is on creating beer rather than technology and information technology, there is a very real potential that someone may make a human error and cause the website to go down. In that instance, a website backup would be really beneficial. A working backup could resolve the issues caused by updates. If the website's corruption was caused by an upgrade, the company's backup could have been extremely useful in restoring the site's functionality and preventing loss of business when the website is down.

Aside from this, there are additional advantages to maintaining a website backup. It could prevent the loss of data, handle compatibility issues when they occur, resolve any malware infections, and protect against any potential hackers.

There are certain PCI DSS requirements that need to be followed to develop a secure website and to avoid these potential pitfalls in future

- Develop internal and external software applications based on industry standards and best practices and also incorporate information security throughout the software development cycle.

- Review custom plugins, extensions, and third-party integrations prior to release to production to identify any potential coding vulnerabilities. This can be achieved by following a code review cycle and identifying the code vulnerabilities.

- Follow the change control process to make any changes to the system components. This change control process is generally implemented by separating development,

and test environments from a production environment. Documenting the impact of changes and by testing the functionalities that the change does not impact the systems.

PROTECTING CARDHOLDER DATA

Businesses must make sure that the Cardholder Data Environment in which sensitive information is managed, stored, or transmitted is completely secure. According to the PCI-DSS Compliance perspective and the security perspective, The security of Cardholder Data should be a top priority for every firm dealing with Cardholder Data.

ACME Brewing and Pub lacks the standards and policies to protect the cardholder's data. Despite the customer accusation of the data leak, ensuring data protection and security implementation around the Cardholder Data Environment is mandatory. The company's culture should change from treating these as common operational issues and should own up to more responsibility for securing customers' data. The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all the firms that accept, process, store, or transmit credit card information maintain a secure cardholder data environment.

ACME Brewing and Pub should satisfy the following requirements and guidelines to protect the cardholder data.

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.
- Protect stored cardholder data by all measures.
- Encrypt while transmitting cardholder data across open, public networks.
- Use and regularly update antivirus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know basis.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

To assess their current risk exposure, ACME brewing and pub must evaluate and scope their Cardholder Data Environment. The likelihood of their organization experiencing data breaches will be determined by scoping and assessing the Cardholder Data Environment. Depending on whether the Cardholder Data Environment (CDE) is minimal or extensive, the systems, applications, and networks that accordingly fall in the scope of PCI DSS, need to be secured by the above guidelines.

ACME Brewing and Pub should shift their business priorities to protect data and include cyber security measures in their daily activities. In addition to the issues reported, there could be many security issues in the company. Following the best practices and standards of cyber security can protect the customer and employees' privacy and in turn, contribute to the positive growth of the business.

WORKS CITED

Joe Tidy, "Twitter hack: Staff tricked by phone spear-phishing scam" *BBC News,* 31 July 2020, https://www.bbc.com/news/technology-53607374

Brad, "Phishing Case Studies: Learning From the Mistakes Of Others" Phishing Protection, 25 March 2021, https://www.phishprotection.com/blog/phishing-case-studies-learning-from-the-mistakes-of-others/

Michael Daniel, "Smarted Cybersecurity Thinking: Change your Mindset to Even the Odds" Cyber Threat Alliance, 25 January 2018, https://cyberthreatalliance.org/smarter-way-think-cybersecurity-change-mindset-even-odds/

Richard Levick, "Change In Corporate Mindset Needed To Combat Cyber Attacks" Forbes.com, 13 February 2017, https://www.forbes.com/sites/richardlevick/2017/02/13/change-in-corporate-mindset-needed-to-combat-cybersecurity/?sh=6aee773017cb

Nicholas Patterson, "What is cyber security and Why is it important" Southern New Hampshire University, 03 December 2021, https://www.snhu.edu/about-us/newsroom/stem/what-is-cyber-security? (snhu.edu)

"7 Main Reasons Why Website Backup Is So Important" 24 September 2021, https://www.strikingly.com/content/blog/website-backup/

Narendra Sahoo, "How to Secure the Cardholder Data Environment and Achieve PCI Compliance" 03 May 2021, https://www.paymentsjournal.com/how-to-secure-the-cardholder-data-environment-and-achieve-pci-compliance/ (paymentsjournal.com)