WHAT YOU NEED TO KNOW ABOUT CYBERSECURITY RISKS

THE DATA DIVA

DATA PRIVACY +DATA PROTECTION +TECHNOLOGY

SEPTEMBER 2023

MISSED OPPORTUNITIES THAT INCREASE CYBERSECURITY RISKS FOR ORGANIZATION

SPONSORED BY ID AGENT

BY DEBBIE REYNOLDS "THE DATA DIVA"

MISSED OPPORTUNITIES THAT INCREASE CYBERSECURITY RISKS FOR ORGANIZATIONS

BY: DEBBIE REYNOLDS

In today's hyper-connected world, Cybersecurity is not just a concern for technical professionals but a critical aspect of any organization's overall cybersecurity health. However, too many organizations miss key opportunities to strengthen their cybersecurity postures, which significantly increases their cybersecurity risks. We will highlight the often overlooked areas that can dramatically heighten Cybersecurity vulnerabilities, which present missed opportunities to reduce cybersecurity risks. This article will discuss three key areas of missed opportunities, including emerging threats, complacency, and employee involvement, and how organizations can turn these missed opportunities into risk-reducing actions.

Being Unaware of Emerging Threats Increases Cyber Risks

One of the most significant Cybersecurity pitfalls for any organization is the lack of awareness about emerging cyber threats. For example, an often-used cyber tip is to look for misspelled words in phishing emails, but guess what? Cybercriminals use spell check just like we do! Cyber adversaries continually evolve their tactics, techniques, and procedures. They adapt to new security measures, adopt new technologies, and find ways to infiltrate even the most secure environments. The FBI's 2022 Internet Crime Report lists phishing attacks as the number one crime reported, with a total loss due to phishing exceeding $103 billion dollars.

Failing to keep up-to-date with such information can have devastating consequences. Ignoring or underestimating the significance of emerging threats can leave an organization unprepared and vulnerable. Even the most robust cybersecurity infrastructure becomes ineffective if it isn't continuously updated to meet new challenges.

How to turn missed opportunities related to emerging threats into Cybersecurity risk-reducing action:

- Subscribe to cybersecurity newsletters, threat feeds, and bulletins to stay informed about new types of attacks or vulnerabilities
- Conduct frequent awareness campaigns for employees to educate them on the latest cyber threats and best practices in cybersecurity
- Develop and regularly update a comprehensive incident response plan to quickly and effectively manage any security incidents

Assuming Cybersecurity Threats Will Not Happen to Your Organization Increases Cyber Risks

Another common misstep is the assumption that cyber threats will not happen to your organization.

Often referred to as the "it won't happen to me" syndrome, this mindset leads to a lax approach to cybersecurity measures. Also, with more cyber attackers using advanced methods and automation, there is no target too small or large to be the target of a cyber attack. Many organizations that felt invincible or felt they were too small to be a target have fallen victim to attacks, costing them not just money but also their reputation and sometimes their businesses. It is essential to consider that every organization —regardless of size, industry, or location—is a potential target. Adopting a proactive rather than a reactive approach can be the difference between a manageable incident and a full-blown crisis.

How to turn missed opportunities related to complacency into Cybersecurity risk-reducing action:

- Encrypt sensitive data both at rest and in transit to protect against unauthorized access
- Have a clear protocol for what to do in case of a security breach, and conduct regular drills to ensure staff are familiar with it
- Give employees access only to the information they need for their roles, reducing the potential points of entry for cybercriminals

Not Including Employees in Actionable Cybersecurity Activities Increases Cyber Risks

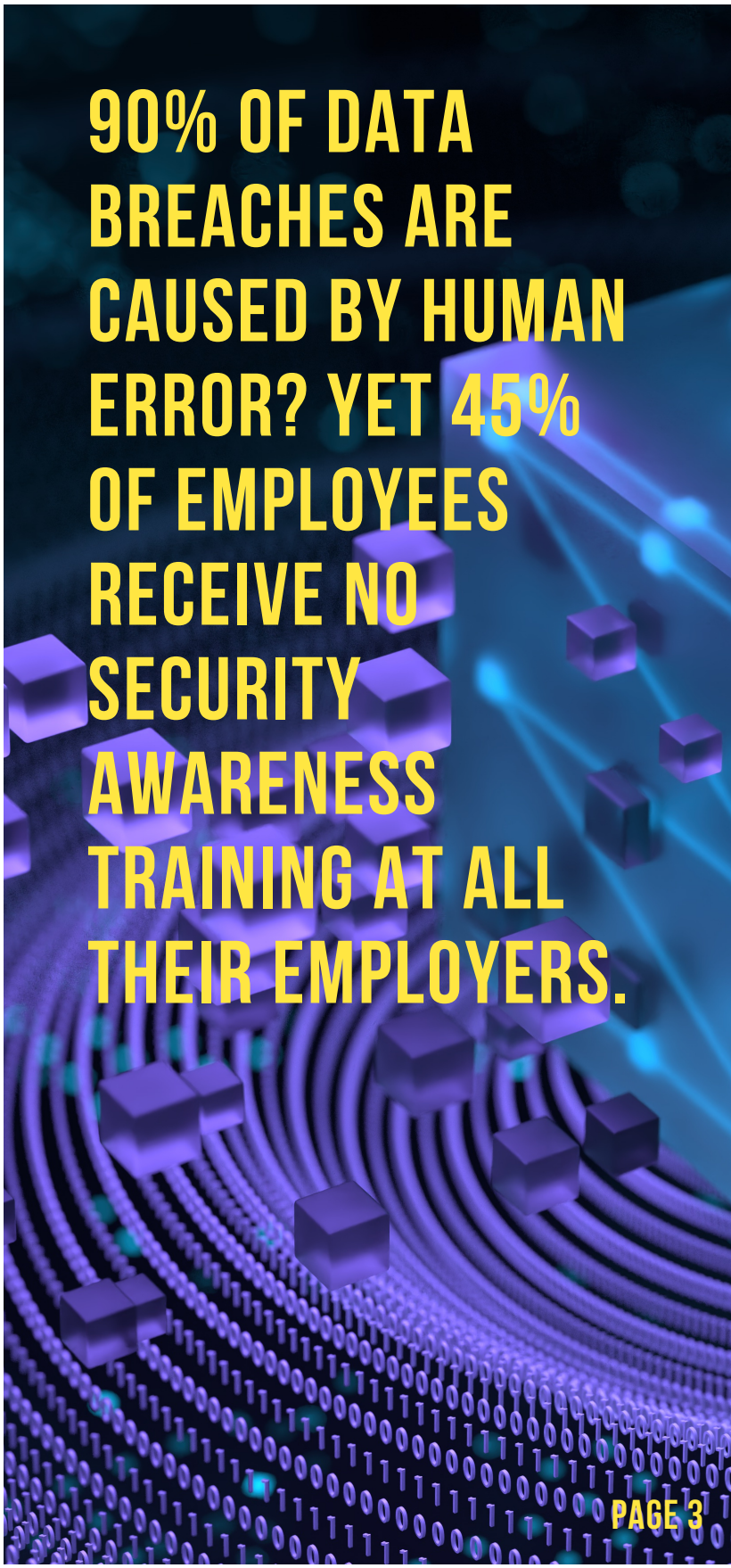
Did you know that over 90% of data breaches are caused by human error? Yet 45% of employees receive no security awareness training at all their employers. Employees are often considered the weakest link in an organization's Cybersecurity chain. Yet, surprisingly, many organizations do not include them in actionable cybersecurity activities. Instead of seeing employees as a potential risk, it's time to view them as the first line of defense. Failure to include employees in cybersecurity efforts can result in uninformed staff making errors such as clicking on phishing links or using weak passwords. Simple mistakes can have a snowball effect, leading to more significant breaches. On the other hand, an informed and educated employee base can act as a robust security layer equipped to identify and report potential threats before they escalate.

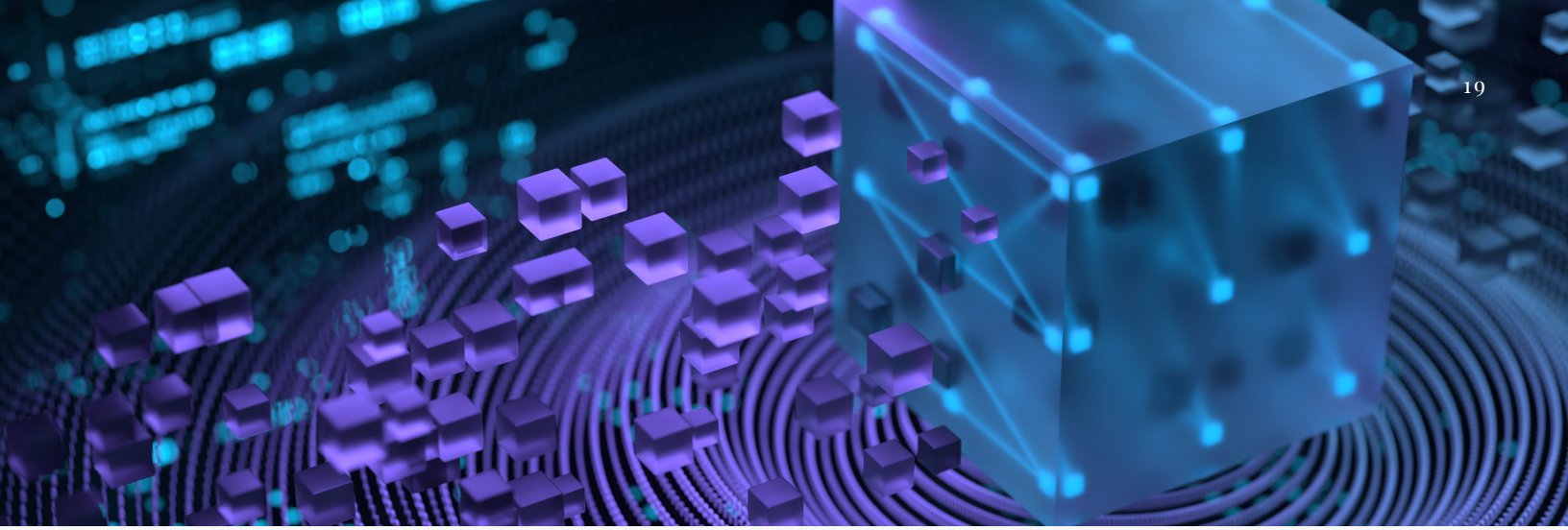
How to turn missed opportunities in employee engagement into Cybersecurity risk-reducing action:

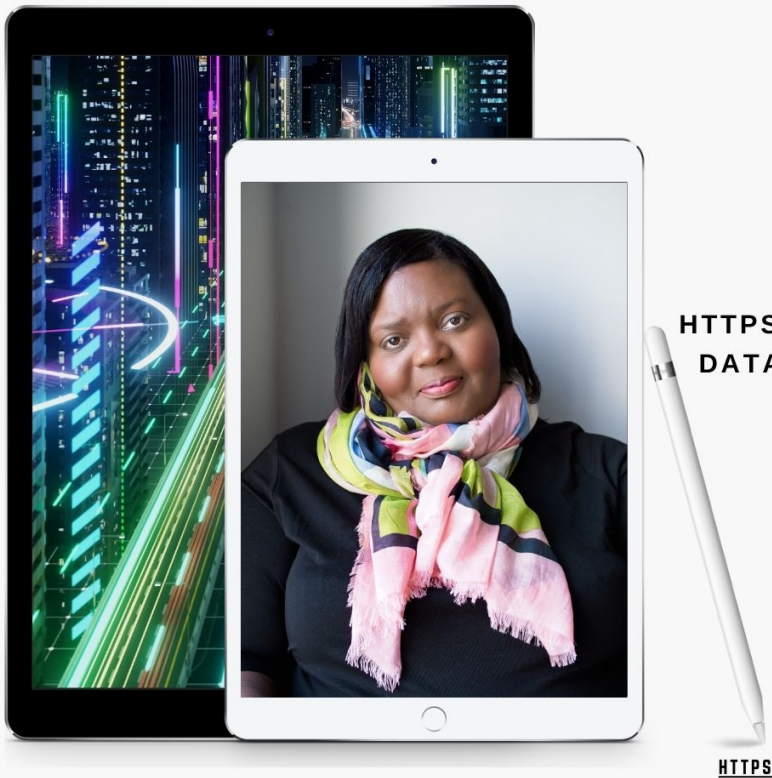
- Implement simulation cybersecurity training sessions for all employees to educate them on role-playing with cybersecurity scenarios
- Create an easy-to-use system for employees to report suspected cybersecurity threats
- Reward employees who identify and report cybersecurity issues, encouraging a proactive cybersecurity culture

Ignoring emerging threats, assuming that cyber-attacks won't happen to your organization, and neglecting to include employees in actionable cybersecurity measures are all missed opportunities that increase cybersecurity risks.

Organizations must adopt a more comprehensive and proactive approach, focusing on continuous education, awareness, and preparedness, to effectively mitigate these risks. Being vigilant and taking these often-overlooked factors seriously can make all the difference in safeguarding an organization's digital assets.







CONTACT US

DEBBIE REYNOLDS

DEBBIE REYNOLDS CONSULTING, LLC

HTTPS://WWW.DEBBIEREYNOLDSCONSULTING.COM

DATADIVA@DEBBIEREYNOLDSCONSULTING.COM

+1-(312) 513-3665

HTTPS://WWW.LINKEDIN.COM/IN/DEBBIEAREYNOLDS/

HTTPS://WWW.YOUTUBE.COM/CHANNEL/UCVZ2NIE9BW43AH1QZVJH2UQ/VIDEOS

HTTPS://THEDATADIVATALKSPRIVACYPODCAST.BUZZSPROUT.COM/

About the Author: Debbie Reynolds, "The Data Diva," is a leading voice in Data Privacy and Emerging Technology. With 20+ years of experience, she is a trusted advisor and thought leader in industries such as AdTech, FinTech, EdTech, Biometrics, and IoT. As CEO of Debbie Reynolds Consulting LLC, she combines technical expertise, business acumen, and advocacy. She is a sought-after speaker, media personality, and recipient of numerous honors and awards, including the host of the #1 global award-winning “The Data Diva” Talks Privacy P, a spot in the Global Top Eight Privacy Experts, and the Global Top 30 CyberRisk Kop Communicators.

Read the eBook “Security Awareness Upgraded: Enter the Simulation” to learn more: https://bit.ly/44QvxJm

Request a demo: https://bit.ly/3Psn2Qa

This post was sponsored by ID Agent, but the opinions are my own and don’t necessarily represent positions or strategies of ID Agent.