THE IMPACTS OF A BREACH

A review of the latest security threats and how you can avoid them

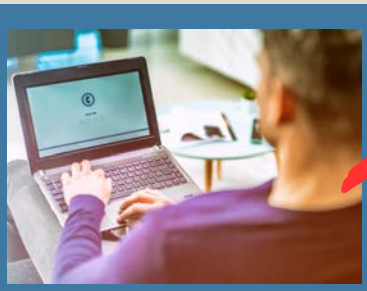
THIS MONTH'S TOPICS:

Many large breaches or cybersecurity incidents make the news, but we really only get a snapshot of the many **ripple effects** caused by that one event. There's the employee who caused the breach, the breached company and management, and not to mention the individual whose information was exposed.

These events can be very damaging to all those affected parties. Financial issues, job concerns, emotional damages, and more could plague an individual and have lasting effects after a breach. Although troubling, these impacts highlight the necessity of your ongoing training. By doing your part of cybersecurity diligence and reporting any security concerns to your supervisors or IT, you can help limit or eliminate these negative impacts of a breach.

The Impacts of a Breach

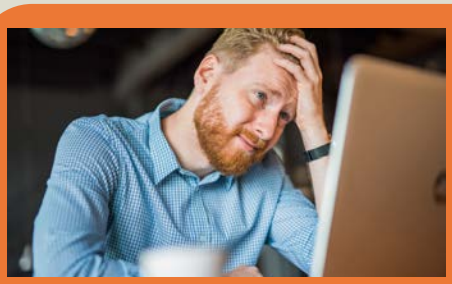
Breaches can have a major ripple effect of consequences. It's not just the individual at fault who may suffer, but the company, managers, and customers who all could feel the impact. Let's review a story of an incident and see all the negative consequences that stemmed from it.



Eugene worked in the finance department at Arcadia Tile and Flooring. One Friday afternoon, Eugene received an email from their billing software that his password had expired and he needed to set a new one. He clicked the link and arrived at a webpage where he provided his current email and password, then set a new password.

After completion, Eugene went on with his day. A few hours later he tried to log into his billing account with his newly set password, but was denied. He tried his original password but that too was not allowing him entry. He thought something might have been wrong but decided to look into it more on Monday and left for the weekend.

Eugene had unknowingly provided his login credentials to a cybercriminal through a fake webpage that was set up and linked in the fake email. The cybercriminal had many days of unfiltered access to Arcadia's billing platform to steal customer billing information until Eugene finally spoke up about his issues with his supervisor.



The Impact for Eugene - The Employee at Fault

Because Eugene caused the large breach for Arcadia, he was immediately fired. Eugene spent time finding a new job but struggled when he had to explain why his last position ended. Companies were fearful of hiring Eugene because of his past as they worried his errors could carry over to them. This caused Eugene a lot of emotional stress, and guilt.

How this could impact YOU: Cybersecurity should be taken seriously, as one simple mistake can affect your current and future job opportunities.

Key Takeaway: Pay extremely close attention to emails, text messages, and phone calls you receive. But if you do think you've caused an incident like this, tell your supervisor or IT as soon as possible.

The Impact for Crystal - Eugene's Manager

Crystal is a top executive at Arcadia Tile and Flooring. After Eugene's incident, it was discovered that Crystal turned down an offer for phishing training for all staff. She thought they would be able to spot these scams but it only took one click for her to be proven wrong. Though on thin ice, Crystal still kept her job, but this is expected to have seriously hurt her chances for a future promotion.

How this could impact YOU: For those that directly manage others, you may be responsible for their actions in a cybercrime event. This could affect your job, bonuses, or promotion opportunities.

Key Takeaway: Take the training of your employees seriously. Encourage participation in cybersecurity education for all staff; we are only as strong as our weakest link.

The Impacts of a Breach - Continued

The Impact for Arcadia Tile and Flooring
Management at Arcadia quickly went into crisis mode, trying to clean up Eugene's mess. Arcadia had to pay for digital forensics, legal fees, and credit monitoring services. These expenses and more left a large bill, expansion plans and new job openings were postponed, and bonuses were canceled.

How this could impact YOU: Even if you didn't cause the breach, a situation like this at your company can directly impact you. It is not uncommon to see employee layoffs, bonuses, and company events canceled, or even a complete company closure in serious situations.

Key Takeaway: Encourage your coworkers to participate in their trainings so we are all gaining cybersecurity awareness. Managers should ensure that incident response plans are in place and cyber insurance plans should be strongly considered.

The Impact for Maria - A Breached Customer
Maria received a letter describing the incident at Arcadia Tile and Flooring and that her financial information may have been exposed. Although Arcadia offered credit monitoring, Maria took an extra step and got new bank cards and put a credit freeze on her account. She constantly receives scam phone calls using her information found in that breach.

How this could impact YOU: Being involved in a breach is not your fault but can be damaging. If financial information was exposed, there could be major implications to your finances. In addition, other information obtained about you can be used for advanced phishing and phone scams.

Key Takeaway: You can't prevent a breach from happening with your information, but be proactive by continuously checking your credit and bank information, accepting credit monitoring services offered by the breached company, and watch for future scams.

WI-FI ROUTER SECURITY

A Wi-Fi Router is used to distribute your internet connection throughout your home or office. This critical piece of technology is a necessity for connectivity, but can present a major security risk if not properly configured. Consider these tips for securing your Wi-Fi router:

Change the passwords - This includes the network password used by devices to connect and the admin password used to access the important administration page.

Keep the router up-to-date with software and firmware updates. Try setting up alerts or automatic updates.

Consider upgrading - Older routers may not have as many security features. Try upgrading to a newer model.

Enable WPA2 or higher encryption - This will scramble traffic going in and out of your router and require each new device to enter the password to connect.

SCAM OF THE MONTH

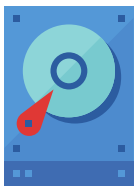
Each month we highlight a REAL scam that was submitted to our security team. We highlight these real examples of tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Diego is trying to upgrade his laptop which meant getting rid of his old laptop. Diego bought this laptop himself a few years ago and used it for work from home activities during the pandemic. He put an ad in a social media public marketplace with the advertisement, "Selling my faithful work laptop, still works! I'll clear all the company data when sold." Diego's ad got a lot of hits and he soon had a buyer at his door. Before the buyer paid, she asked Diego if the device still had his work information on it. Diego said yes, but he would clean it off.
Diego received the cash and said to the seller he would just need a few minutes to wipe the hard drive. The buyer said she was in a bit of a rush and would take care of that herself. The buyer did not wipe the drive and resold the laptop on the Dark Web.

Did you spot the red flags?

- Diego didn't check with his supervisor before selling this device he used for work.
- Diego advertised the computer was used for work, and had company data, attracting a shady buyer.
- The buyer insisted they would clear the data for Diego.

Disposing of devices properly is very important. These devices we use on a daily basis can store massive quantities of sensitive information. If the data is not properly wiped from a device, it could be easily accessible to the next person who obtains it. Even your personal devices will store **YOUR** sensitive information that you wouldn't want others to have.



A device's hard drive is generally where information is stored. When the time comes for disposal, this information could be **deleted**, **overwritten**, or the hard drive itself could be **destroyed**. Electronic devices that should be considered for proper disposal include computers, smartphones, tablets, USB drives, and other backup media.

Always **check with your supervisor** before disposing of a piece of equipment used for work purposes. Yes, it may be a device you purchased, but if there is a chance sensitive work data is residing on the device, management and IT should have a chance to remove that information securely.

Preventing a Breach's Domino Effect

Key Takeaways

There are many consequences from breaches that affect various parties. Take these threats seriously to help lessen the chance of one of these events occurring.

Breaches can have serious ripple effects on many individuals. The employee at fault may be fired and have difficulties obtaining a new position, the company involved will suffer some severe financial issues, and the individuals whose information was exposed may be at risk of more scams or financial woes.

Protect your Wi-Fi routers. These terminals can act as a gateway into your home or office. Lock them down from intruders with strong passwords, encryption, and keep them patched and updated.

Make sure you are following proper disposal procedures set up by your organization. Be aware that personal devices may have some work information and should be properly wiped before being sold or disposed of.

Cybersecurity Anagrams

Some key words have been scrambled below. How many can you get without cheating?!

1. Specials Voided d _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
2. Recite Your Rust _ _ _ _ _ _ r _ _ _ _ _ _ _ _ _
3. Sconce Queens _ _ _ _ _ _ _ _ u _ _ _ _ _ _ _ _
4. Loafers _ o _ _ _ _ _ _ _ _
5. Replay Meat _ _ _ _ m _ _ _ _ _ _ _ _ _ _ _
6. Had Driver _ a _ _ _ _ _ _ _ _ _ _ _
7. Flyleaf Moose Yep _ _ _ _ _ _ _ y _ _ _ _ _ _ _ _ _ _ _ _
8. Wide Apart Femur _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ d _ _ _ _ _ _ _ _ _ _

Answers: 1. Disposal Procedure 2. Router Security 3. Consequences 4. For Sale 5. Team Player 6. Hard Drive 7. Employee Layoffs 8. Firmware Update