WHEN IT RAINS, IT POURS

Examining the splash back of a breach on a company

THIS MONTH'S TOPICS:

Light Drizzle

Small businesses and breaches...

Monsoon Season

Large businesses and breaches...

Scam of the Month:

It's raining scams...

Cyber Zen Den:

The calming sounds of rain...

April likes to rain a lot, and scammers like to scam a lot.

So what happens when you're unaware of today's weather, and you venture out, sans umbrella? The same thing that's likely to happen when you're un-cyberaware, surfing the internet: you get drenched, and it's not pretty.

Companies large and small have suffered the effects of being caught up in a cyberscam. Studying these events can provide insights into the events leading up to, and resulting from a breach.

And maybe, just maybe, these cautionary tales will remind you of the importance of bringing your cyberawareness-umbrella next time you're on the internet.

60% of small companies go out of business within six months of a data breach or cyber attack.

How does this happen?

For one small hotel business, this cyber-storm began when hackers gained access to the owner's email account.

- The hackers were then able to view the owner's calendar.
- While the owner was in meetings, the hackers contacted his bookkeeper.
- Impersonating the owner by mimicking previous messages, the hackers requested that the bookkeeper transfer money into a new account.
- By the time the heist was discovered, over $550,000 had been lost.
- The bank refused to reimburse the losses, and the owner sued, draining further resources.

Research shows that 43% of cyberattacks are aimed at small business, with most breaches caused by successful phishing attempts.

Yet only 14% of such businesses prepare themselves, and their staff for the rain.

Big Business Breach

How small errors escalate

Repercussions

When breaches occur, the business may incur costs such as mandatory credit monitoring for compromised customers, identity theft repair, and additional compliance requirements. Affected customers may lose trust in the company, and the breach may be blasted on media outlets, tarnishing potential customer's opinions. Depending on the situation, the employee at fault can be placed on warning, receive mandated training, or be let go.

PII Harvest

This information can be sold on the Dark Web for buyers to commit identity theft or easily access personal accounts.

Malware

When installed, scammers can access files, or watch computer actions, in order to steal personal details and commit fraud.

Laptop

A laptop theft occurs every 53 seconds. Whether it's stolen from the office, or public transportation, such loss of a work device can lead to a severe breach.

Cell Phone

Studies show that the cause of many current breaches is due to employees using their mobile devices to access company information.

Desktop

Experts warn against weaving personal and professional lives on work provided device, as this increases the probability of a breach.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, that way you'll be better prepared when the next scam hits.

Dennis started a new job at a local university. He received cybersecurity training as part of his onboarding, but he didn't pay much attention. He's received similar training in the past and knows all about strong passwords and what to look out for in a phishing email.

Dennis's third week of work was during finals. Students were cycling in and out of his office, and coworkers were blowing up his email. In between meetings with students, he would go through his inbox as quickly as he could, skimming over content and prioritizing tasks that would take the least amount of time.

When Dennis came across an email asking him to confirm his new account, he clicked the confirmation button, plugged in his credentials (which were the same across all his university accounts), and filed the email away as another task completed.

Soon after, the university experienced a ransomware attack. The the networks were compromised and rendered the school Wi-Fi unusable. They were forced to cancel all online and hybrid classes, and finals were forced to be extended, impacting graduation.

Did you spot the red flags?

- Dennis didn't pay attention to his onboarding because he thought he knew the content, but such training could have provided him with university specific cybersecurity best practices
- Dennis used the same credentials across all university platforms, even though he claimed to have known about strong passwords. There is a difference between knowing, and doing, and in order for cybersecurity training to be effective, the knowledge learned must be put to use in order to protect data.

In academia, it is often the responsibility of IT to provide privacy governance, but a community culture that emphasizes everyone's duty to protect data would help serve all organizations.

Universities face a unique vulnerability with a large portion of their users living "on site," and experiencing high turnover. Addressing concerns that are specific to a company's niche could prevent scammers from targeting such weaknesses.

For universities, January and May sees a peak in cybersecurity incidents. This is during finals when students and staff are busiest. Other institutions may also find that their busy season corresponds with an increase in unintentional data disclosures.

Key Takeaways

Businesses big, small, and specialty all have their own unique plight when it comes to cybersecurity. Still, regardless of business size and type, a single, small mishap can result in dire repercussions.

It is every employee's responsibility to remain cyberaware while on and off the job, putting their cybersecurity training into practice, and understanding the consequences of their own actions within their field.

Small businesses lay it all on the line: With less resources to help pull them out of a breach, small businesses take bigger risks when they don't have the cybersecurity structures in place to prevent attacks.

More resources, more responsibility: Big businesses house the PII of thousands of people who trust the company to protect their information. With so many devices, and so many employees, big businesses need to stay on top of all the ways their data can be attacked.

Practice what you preach: Just knowing cybersecurity information protects no one. Put this knowledge into practice in order to keep your business safe.

The Calming Sounds of Rain

Rain has a regular, predictable, and not-threatening pattern of sound that has been known to soothe and calm.

How does this relate to cybersecurity?

During any sector's busy season, employees often find themselves under stress and tight on time. This can often lead to needless mistakes being made. But, on a rainy day, have you ever noticed that the office collectively slows down, the work noise is quieter, and a lot of that stress seems to melt away?

Now apply this concept to cyber-awareness.

When work becomes overwhelming, and you feel your error-prone mindset kicking in, take a moment to listen to the rain (either real or artificial). Let the rhythmic tapping envelop you until you feel more at peace, and ready to work with a calmer state of mind.