MEL CYBER TASK FORCE UPDATE

Anatomy of a Data Breach: What are They & What to do When You Spot One?

Arguably no phrase has dominated the tech world the last 24 months more than the term “data breach.” From breaches that have impacted critical infrastructure like the Colonial Pipeline to hackers compromising healthcare records at UC San Diego Health, the last two years have been saturated by headlines of cybersecurity mishaps. Yet, despite the prevalence of the breach-centric newscycle, many everyday individuals may not know what exactly a data breach is, how they typically start, and why they occur.

According to IBM, the average time it takes to identify that a breach has occurred is 287 days, with the average time to contain a breach clocking in at 80 days. And with 81% of businesses experiencing a cyberattack during COVID, it is essential that individuals are familiar with the anatomy of a data breach so that they can keep their data, as well as their colleagues and customers’ data, safe.

With that in mind, here is some helpful background on what data breaches are and why they are so problematic.

What is a data breach?

While it may seem like a complex concept, once the jargon is removed, a data breach is actually really straightforward to explain. According to Trend Micro, a data breach is “an incident where information is stolen or taken from a system without the knowledge or authorization of the system’s owner.” And while data breaches can be the result of a system or human error, a vast majority of data breaches are the result of cyber attacks, where a cyber criminal gains unlawful access to sensitive system data. In fact, 92% of the data breaches in Q1 2022 were the result of cyberattacks.

What kind of data can be breached?

Unfortunately, cyber criminals look to get their hands on any information that they possibly can ranging from more obvious sensitive information such as social security numbers and credit card information to more obscure data like past purchase history.

MEL CYBER TASK FORCE UPDATE

What are some of the tactics used to execute data breaches?

Cybercrime is getting more sophisticated each day. However, cyberattack tactics do not have to be cutting-edge or advanced in order to be very effective. Here are a few examples of popular tactics used by cybercriminals:

- **Phishing**: Phishing is when a cybercriminal pretends to be a legitimate party in hopes of tricking an individual into giving them access to personal information. Phishing is one of the oldest tricks in the book for cybercriminals but it is just as effective as ever. For example, 80% of security incidents and 90% data breaches stem from phishing attempts.
- **Malware**: Another tried-and-true method for cybercriminals is malware. Malware is malicious software that secretly installs itself on devices – often by way of a user engaging with fake links and content – and quietly gains access to the data on an individual's device or a business network.
- **Password Attack**: Through password attacks, cybercriminals look to gain access to sensitive data and networks by way of "cracking" user passwords and using these credentials to get into networks and extract data from a given network.

How to spot a possible breach?

The best way to stop a data breach is to stop it before it even starts. This includes taking steps from making sure passwords are long and complex to reporting suspicious emails. If you do suspect that you have been the victim of a breach immediately contact your IT department or device provider to notify them and follow subsequent protocols to help them scan, detect, and remediate any issues that exist.

For more information about cyber risk control, model policies, cyber insurance, news, tips and best practices visit NJMEL.org.

For details, contact the MEL Underwriting Manager or your local JIF Executive Director

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND · MEL · MEL