CYBERRISKS&LIABILITIES_

Doxxing

In this day and age, the amount of information being stored online is constantly increasing. Some of this information may be confidential, and some may be so sensitive that a data breach could threaten the future of your business.

"Doxxing" is a type of cyber attack that results in the collection and exposure of sensitive information that could damage the credibility or reputation of a person or an organization. In doxxing, the criminal's goal is to breach, collect and expose documents, often abbreviated as "docs." This is usually done with the purpose of either harassing, blackmailing or embarrassing the victim. Sometimes, doxxing may even be part of the hacker trying to get revenge or incite physical harm.

As cyber criminals become more sophisticated, it is clear that anyone can be targeted, whether they be ordinary citizens, law enforcement agents, politicians or business leaders.

Your Business at Risk
Companies of all sizes are at risk of being the target of cyber attacks. Good cyber security practices are always important for protecting your employees' information, confidential company files and sensitive details about your partners or clients.

But, when it comes to doxxing, it's your leaders who are most likely to be targeted by attacks. One of the most effective ways to embarrass a business, or harm its reputation, is by exposing negative information about one of its leaders. If embarrassing details about a leader in your organization come to light, even if they have nothing to do with the actual business practices of your company, the effects can be devastating.

How It Works
There are a number of ways that doxxers may be able to gain access to sensitive information. Some common sources include:

- **IP addresses**—All devices connected to the internet have an IP address, which can then be tracked with an IP logger to track online activities and locations.
- **Data brokers**—Data brokers purchase customer lists from other businesses that you may have provided your information to, such as airlines or subscription services.
- **Domain sales brokers**—Registration information used to create a website can be accessed through domain sales brokers or the WHOIS database. This is especially noteworthy for organizations that have created their own website.

In a doxxing attack, the attacker may use any one of a number of possible methods. These can vary greatly and include using the aforementioned IP logger, breaching the security of a Wi-Fi network, stalking social media profiles or even using cellphone numbers to learn personal information.

Cyber Security Practices
When it comes to protecting your company's data and reputation, things naturally start with implementing, explaining and enforcing good cyber security practices.

To keep your business as safe as possible from a possible doxxing attack, implement the following policies:

- Require strong passwords with a variety of letters, numbers and special characters.

Conrey INSURANCE BROKERS & RISK MANAGERS

- Use a variety of passwords across different platforms.
- Instruct employees to avoid connecting devices to untrusted or unprotected Wi-Fi networks.
- Keep software on devices updated, and avoid installing any unapproved software.
- When possible, use VPNs in order to conceal IP addresses.
- Instruct employees to avoid suspicious websites, be wary of phishing emails and avoid using their work email for personal reasons, such as subscription services.

These policies should be followed by all employees, including leadership, whether they are working at the office, remotely, with company computers or personal devices.

Social Media Awareness
In addition to hackers continuing to improve their methods of attack, many of their targets have simultaneously been making things even easier for cyber criminals. With social media being a part of everyday life, it has also led to vulnerability for people who are too willing to share personal information online. Oftentimes, these people do not realize that such information can be used against them.

It is important that you advise leaders in your company to increase their privacy settings on social media, or to limit the amount of information that they share to begin with. Instruct your employees to avoid allowing just anyone to view their social media pages and to limit "friends" to people who they actually know in real life and are confident would not attempt to do them harm. When it comes to doxxing, allowing just anyone to see your address, phone number, email or even place of employment can help hackers wedge their way into the private details of your life.

Employees should think twice about how much information they share, even with people they think they can trust. It may be a good idea to have employees look themselves up on a search engine, as they may be surprised by how much information is actually out there and completely public.

The process of looking oneself up on the internet and then having potentially sensitive or vulnerable information deleted is often referred to as "self-doxxing" and can greatly decrease the risk of an attack.

High Stakes
There is no shortage of examples of organizations suffering huge financial losses and severely damaged reputations due to a leader bringing about embarrassment.

Even if the victim of the attack has done nothing wrong that directly associates with their job or your company, disreputable information about their personal life can still cost you dearly.