Cyber Risks & Liabilities

Third Quarter 2019

3 Ways to Protect Yourself From Credential Stuffing

Credential stuffing attacks occur when a malicious party takes a stolen username and password, and tries them on a variety of different websites. For example, a hacker may have purchased a Google username and password from the dark web. Assuming that you use the same password for multiple accounts, the hacker would test these credentials on other platforms (e.g., banking or social media websites) using botnets (groups of computers tasked with various commands).

Essentially, by using information from one account, criminals can potentially access data from a variety of platforms, draining bank accounts or gathering information they can sell to other malicious parties.

Credential stuffing can affect anyone, from individual users to the biggest companies. Thankfully, because credential stuffing relies on victims having the same password for multiple accounts, there are some simple ways to protect yourself:

1. **Avoid using the same password for multiple accounts**—Credential stuffing works because many people use the same password for multiple accounts. To avoid becoming a victim, it's important to change your passwords often and use a unique password for each account.
2. **Use two-factor authentication**—While complex passwords can deter cyber criminals, they can still be cracked. To prevent cyber criminals from gaining access to your accounts, two-factor authentication is key. Through this method, users must confirm their identity by providing extra information (e.g., a phone number or unique security code) when attempting to access corporate or personal applications, networks and servers. This additional login hurdle means that would-be cyber criminals won't easily unlock an account, even if they have the password in hand.
3. **Create strong password policies**—For employers, ongoing password management can help prevent attackers from compromising your organization's password-protected information. You'll want to create a password policy that requires employees to change their password on a regular basis, avoid using the same password for multiple accounts and use special characters. Long passphrases are becoming increasingly popular as well.

Even the most robust and expensive data protection solutions can be compromised should an employee click a malicious link or download fraudulent software. As such, it's critical for organizations to thoroughly train personnel on common cyber threats and how to respond.

Robertson Ryan & Associates
800.258.0277
www.robertsonryan.com

ROBERTSON RYAN
& ASSOCIATES

Cyber Incidents Cost More Than You Might Think

As technology advances, companies are collecting, storing and transferring more personal information about their customers and employees than ever before. This not only opens organizations up to a cyber attack, but it also means that just one breach can affect thousands or even millions of individuals. And, unfortunately for organizations, cyber incidents cost more than just data:

- **Data breaches are becoming increasingly expensive.** While cyber liability insurance can help offset the costs of a data breach and any subsequent litigation, just one breach can be financially devastating. According to a survey conducted by the Ponemon Institute, the average cost of a data breach was $5.78 million, or $255 per lost or stolen record.
- **Litigation and regulatory costs can be significant.** Failing to handle a data breach properly can result in litigation or major fines. One example of this occurred in 2018 where, following a breach from 2013 where 3 billion accounts were compromised, Yahoo failed to disclose any details of the hack for three years. The U.S. Securities and Exchange Commission fined the organization $35 million dollars as a result.
- **Cyber incidents can lead to serious reputational damage, significantly impacting directors and officers.** Reputational damages can easily reach six figures. According to Kaspersky Lab, a global cyber security company, a single cyber incident recently caused brand damage of $8,000 for small and medium-sized businesses and $200,000 for larger organizations. When wide-scale breaches occur, a company's reputation can be tarnished, sometimes permanently. In addition, the public holds organizations accountable for major losses of personal data, and directors and officers are often the ones who take the blame.

To learn about basic cyber security protections and coverage options, contact your broker today.

Mobile Device Security

Gone are the days when the most sensitive information on an employee's phone was the names and phone numbers of their contacts. Now, a smartphone or tablet can be used to gain access to anything, including emails, stored passwords and even proprietary company data. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving a traditional computer system.

In order to protect your organization, there are a number of mobile device security measures to consider:

- **Establish a mobile device policy**—Before issuing mobile phones or tablets to your employees, establish a device usage policy. Provide clear rules about what constitutes acceptable use as well as what actions will be taken if employees violate the policy. It is important that employees understand the security risks inherent to mobile device use and how they can mitigate those risks. Well-informed, responsible users are your first line of defense against cyber attacks.
- **Establish a bring your own device (BYOD) policy**—If you allow employees to use their personal devices for company business, make sure you have a formal BYOD policy in place. Your BYOD security plan should also include the following practices:
    a. Installing remote wiping software on any personal device used to store or access company data.
    b. Educating and training employees on how to safeguard company data when they access it from their own devices.
    c. Informing employees about the exact protocol they must follow if their device is lost or stolen.
- **Keep the devices updated with the most current software and anti-virus program**—Software updates to mobile devices often include patches for various security holes, so it's best practice to install the updates as soon as they're available. There are many options to choose from when it comes to anti-virus software for mobile devices, so it comes down to preference. Some are free to use, while others charge a monthly or annual fee and often come with better support.
- **Back up device content regularly**—Just like your computer data should be backed up regularly, so should the data on your company's mobile devices. If a device is lost or stolen, you'll have peace of mind knowing your valuable data is safe.

Because of their convenience, smartphones and tablet devices have become a universal presence in the modern business world. As usage soars, it becomes increasingly important to take steps to protect your company from mobile threats, both new and old.

For more cyber security strategies you can use to protect your businesses, contact Robertson Ryan today.