The Most Common Types of Cyberattacks Plaguing SMBs An How to Protect Against Them

By Richard Clarke, Chief Insurance Officer, Colonial Surety

The media landscape is dominated by headlines like this “Hackers Target Cryptocurrency Companies in HubSpot Data Breach” and this “Microsoft confirms it was breached by hacker group.” Leading most to believe that cyberattacks and data breaches only afflict larger companies. However, the truth is, small and midsized businesses (SMBs) are likely more vulnerable as they generally have less protection, and more limited budgets to address management of the risk.

Most SMB owners don’t know they are just as susceptible to a cyberattack as their larger counterparts. But, in fact, a recent report from IBM revealed that SMBs spend about $3M per breach, underscoring just how important it is for SMBs to take cybersecurity and cyber protection seriously.

In order to understand the actions SMBs should take to best protect themselves, it’s important to first identify the types of cyberattacks they are most likely to face. With that, let’s quickly review three of the more common, ongoing types of cyberattacks facing SMBs.

1. **Cyberextortion and Ransom Demands**. Cyber extortion and Ransom Demands are one of the most common cyberattacks for SMBs. These scenarios involve an attack or threat coupled with a demand for money, or some other response, in return for stopping or remediating an attack. SMBs are particularly vulnerable to these types of attacks because they do not have the protections that larger organizations do, nor do they have the budgets to ramp up their spending in those areas.

2. **Privacy-Related Violations**. Privacy-Related Violations involve a cyberattack or data breach that result in a hacker or cybercriminal gaining unauthorized access to a database or network and stealing private information. Any business that warehouses, handles, or transfers personal or corporate information, has a potential exposure to this type of cyberattack.

3. **Social Engineering Fraud**. Social Engineering Fraud, which can also be known as Impersonation Fraud, is a particularly tricky threat for any sized business. Unlike other common types of cyberattacks that exploit security vulnerability, social engineering fraud targets employees by fraudulently impersonating a third party in an effort to deceive an employee to release funds or property, generally via wire transfer – this is often done through email phishing.

The aftershock

If you think the attack itself is where the problem begins and ends, you would be wrong. Following an attack there are aftershocks that can ripple for decades if a company is not properly prepared.

For instance, Intrusion-Related Restoration Costs. This occurs when an SMB has experienced an attack that includes unauthorized access to their networks. As a result, businesses are tasked with paying steep costs in order to restore their networks to proper operating function. Not only can this process be expensive, but it can be time-consuming as well.

Another example are Notification-Related Expenses. When personally identifiable information is involved in a data security breach, notification laws, which vary state-to-state, require that the affected individuals be formally notified in order to take proper precautions to protect their information. The cost of providing the notifications as mandated by individual statutory laws is an unbudgeted expense for SMBs and can be quite costly.

Setting up the appropriate guardrails

There are actions SMBs can take to both minimize the risk of these types of cyberattacks, as well as to prepare for them if they do occur.

First, check, and re-check, cyber-vulnerabilities on an on-going basis. This can be achieved internally, though some businesses choose to employ the use of ‘friendly hackers’ to help determine their biggest vulnerabilities.

Second, make use of multi-factor authentication (MFA) to protect against phishing, social engineering and password brute-force attacks. This can also help prevent logins from attackers exploiting weak or stolen credentials.

Third, train employees to contact companies directly when receiving unsolicited messages asking about business related information, never provide personal or business information to someone they are not certain is authorized, never enter sensitive information into a webpage before checking the security settings and make use of existent security measures like email filters, antivirus software, and firewalls. Additionally, each employee should be sure to keep all of their software updated.

To supplement the management of risk efforts by the organization, strong consideration should be given to cyber insurance. Cyber insurance is a safety net offering organizations both legal and technical support to move forward with a response plan – ensuring customers and employees remain digitally safe once an attack occurs. SMBs are sought by many insurers - some insurers focus on writing larger risks, or

some of the exposure, and some insurers prefer SMB-sized risks. A variety of insurance coverage is available, and although cyber insurance pricing has been increasing over the past few years, coverage is generally available.

Essentially every business that deals with sensitive information and data is vulnerable to cyberattacks – regardless of size. With cybercriminals rapidly becoming more sophisticated in their tactics, putting forward a holistic cybersecurity plan combining these measures is the best way for SMBs to prepare themselves for an increasingly likely cyberattack.

About the Author

Richard Clarke, Chief Insurance Officer, Colonial Surety . As an insurance industry veteran with more than three decades of experience, Richard is a Chartered Property Casualty Underwriter (CPCU), Certified Insurance Counselor (CIC) and Registered Professional Liability Underwriter (RPLU). He leads insurance strategy and operations for the expansion of Colonial Surety's SMB-focused product suite, building out the online platform into a one-stop-shop for America's SMBs.

Richard can be reached at https://www.colonialsurety.com