FLEETCOR®

Unrisky Business: Survey Says SMBs Invest More in Cybersecurity

October 10, 2022

Source: James Edgar, Chief Information Security Officer

Cybersecurity is top of mind at FLEETCOR, whether it’s protecting internal assets or safely serving external customers. With that in mind, we are celebrating Cybersecurity Awareness Month this October by sharing insights about the attitudes and actions of about 300 SMBs across the U.S. revealed in our annual State of Small and Medium-Sized Business Cybersecurity Report.

Businesses Willing to Spend to Protect Themselves

Most significant, and encouraging, is that while some SMBs lack the expertise to focus on and develop a cybersecurity program, many recognize the risk with 93% planning to increase or at least maintain funding for cyber defense in the last 12 months.

Even though 7% of SMBs have experienced a cyberattack in the past year, 32% are aware of the increase in cyberattacks and factored that into projected spending. Also encouraging, 80% of businesses are implementing software to prevent malware and viruses.

Don’t Forget the Human Factor

Unfortunately, only 40% of the businesses have implemented strong authentication and even less, 23%, have implemented security awareness training. These are critical to mitigating social engineering, phishing and BEC (business email compromise) attacks. These are attacks in which clever criminals trick employees into opening the door and letting them walk right in. No matter how many technical roadblocks you install, your people are your last line of defense.

SEE THE STATE OF SMBs CYBERSECURITY REPORT FACT SHEET

The biggest concern of 56% of the companies surveyed about a cyberattack is loss of profitability and/or disruption to operations, showing they are more worried about ransomware and other destructive malware attacks than customer data protection.

Monetary concerns are indeed well-founded. According to a report by Ponemon Institute, the average cost of a data breach rose to $4.35 million last year, up from $3.86 million in 2020. However, many may not realize that privacy protection regulations and standards continue to multiply, and pressure is increasing on all businesses to safeguard customer data or pay hefty fines, suffer reputational damage, or get tied up in court for years. All the more reason to train employees to spot and stop an attack in progress.

“See Yourself in Cyber”

This is why, appropriately, this year’s Cybersecurity Awareness Month theme is “See Yourself in Cyber.” In other words, educating people on how to be safe online is essential. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the National Cybersecurity Alliance (NCA) recommend everyone take these simple steps to stay safe:

- Think Before You Click – recognize and report suspicious emails
- Update Your Software – act promptly, or better still, turn on automatic updates
- Use Strong Passwords – use a password manager to generate long, random passwords
- Enable Multi-Factor Authentication - something you know (like your password), something you have (like your phone), something you are (like your face or fingerprint)

The results of our new survey are encouraging in that companies appear more concerned about cybersecurity than they did a year ago. That said, they should shore up their technical defenses with an investment in educating their employees to serve as defenders against attacks and not enablers.

###