CARPENTER INSURANCE

"Home For All Your Insurance Needs"

EST. 1935

Cybercrimes Against Small Businesses Decrease, Although Risks Remain

Small businesses and self-employed people saw fewer cyberattacks and data breaches over the past 12 months. Still, significant risks remain for this corner of the economy, according to the Identity Theft Resource Center's (ITRC) 2022 Business Impact Report. The ITRC recently surveyed 450 people who led small businesses or were self-employed about their experiences with cybercrime. The survey found that 45% of respondents experienced a security or data breach between July 2021 and July 2022, a drop from 58% during the previous year. These respondents also incurred lower costs in addressing breaches. Specifically, most businesses lost less than $250,000, while fewer lost between $250,000 and $1 million.

Cybercriminals most frequently targeted customer and employee data, with roughly half of the respondents reporting compromises of both data types. Just over one-quarter reported a compromise of company intellectual property. External threat actors were the most common root cause of data breaches, followed by compromises from remote workers, malicious insiders, compromises from third-party vendors, and human error.

The survey also identified social media as a top concern for many respondents. In particular, half of the respondents reported cybercriminals taking over their social media accounts, and nearly 90% of impacted companies lost revenue as a result. Phishing attacks and mistakenly sharing account credentials with someone pretending to be a friend or customer were the most common causes of account takeovers. Unfortunately, the survey uncovered a worrisome trend in cybersecurity training. Many respondents reported increasing their investments in new security tools, IT workers and IT staff training but are spending less on overall employee training—potentially creating security vulnerabilities.

Contact us for more cybersecurity updates.

Key Elements of an Effective Cyber Incident Response Plan

Through proper response planning, businesses can mitigate potential damages that may arise from cyber incidents. Yet, it's important to note that cyber incident response planning requires coordination across a company. An effective response plan should outline:

- Who is part of the cyber incident response team (e.g., company executives, IT specialists, legal experts, media professionals and HR leaders)
- What roles and responsibilities each member of the response team must uphold during an incident
- What the company's key functions are, and how these operations will continue throughout an incident
- How critical workplace decisions will be made during an incident
- When and how stakeholders and the public (if necessary) should be informed of an incident
- Which federal, state and local regulations the company must follow when responding to an incident (e.g., reporting protocols)
- When and how the company should seek assistance from additional parties to help recover from an incident (e.g., law enforcement and insurance professionals)

- How an incident will be investigated, and what forensic activities will be leveraged to identify the cause and prevent future incidents

Cyber incident response plans should address a variety of possible scenarios and be communicated to all applicable parties. These plans should also be routinely evaluated to ensure effectiveness and identify ongoing security gaps.

The Benefits of XDR

Extended detection and response (XDR) is a cybersecurity solution that offers businesses end-to-end visibility, detection, investigation and response across multiple security layers. XDR is an evolution of endpoint detection and response (EDR)—a cybersecurity offering that continuously monitors threat information and endpoint data to detect and respond to ransomware and other types of malware. However, EDR can only detect and respond to threats inside managed endpoints, which limits the scope of threats that can be detected. In contrast, XDR goes beyond the capabilities of EDR by analyzing all security layers and offering companies a more holistic view of potential threats. By utilizing extended visibility, analysis and response across endpoints, workloads, users and networks, XDR can help businesses reduce their blind spots, detect cyber exposures faster and jump-start threat remediation. Additional benefits of XDR include the following:

- **Greater visibility and context**—Threats that utilize legitimate ports and protocols can often slip past system defenses undetected. With XDR, businesses can see threats on any security layer and better understand how a cyberattack happened, how it spread and who was affected.
- **Improved prioritization**—As cyberthreats continue to rise, it can be difficult for companies to keep up with security alerts. XDR can help prioritize threats by grouping related alerts across the framework and presenting the most important ones.
- **Enhanced automation**—XDR's automation abilities allow businesses to handle a large volume of data and consistently execute complex processes.
- **Elevated response sophistication**—XDR can tailor specific systematic responses to minimize the overall impact of affected endpoints. Further, since XDR is continuously monitoring the technology landscape, it enables companies to respond to threats faster.

In an increasingly complex threat landscape, XDR solutions can provide businesses with flexible and efficient security enforcement and remediation. For more risk management guidance, contact us today.