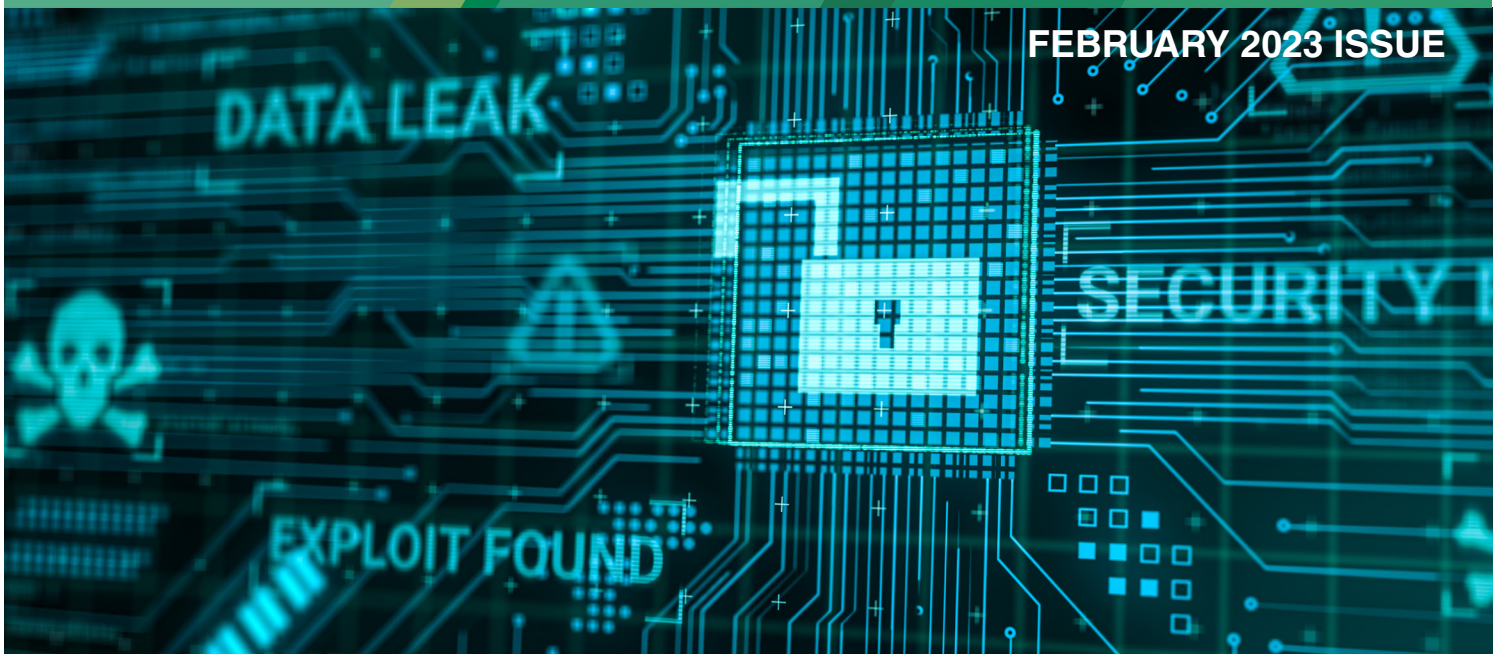
The Logical Advantage

TeamLogicIT®
Your Technology Advisor

FEBRUARY 2023 ISSUE



Technology Trends

Cyber Defense Remains an SMB Priority

Cybersecurity remains among the highest priorities for businesses around the globe as financial damages from cybercrime escalate.

Quantifiable costs like those associated with recovering from data breaches surpassed $6 trillion in 2021 and are expected to continue growing 15% annually, hitting $10.5 trillion by 2025. Moreover, the impact of a company reputation tarnished by losing customer trust is immeasurable.

In sum, falling victim to cybercrime can cripple an organization of any size or type. But the issue is especially vexing for small- to medium-size businesses (SMBs)—a segment that's under increasing cyber assault.

Consider these figures from last year's Comcast SMB cybersecurity report about one day last year:

- Comcast's SMB customers were threatened by more than 70 million instances of malicious bot activity
- During the same period, SMBs weathered 30 million phishing forays
- Attempts to implant malware exceeded 20 million

Lacking the deep pockets of large enterprises, the challenge for SMBs is mounting an adequate cyber defense with limited budgets and fewer expert resources. That's why tech analyst Gartner expects that firms of all kinds will increasingly turn to managed IT services in 2023 as a cybersecurity strategy.

As a top-tier managed services provider (MSP), we take a holistic approach to protecting your business and its data that reaches beyond deflecting assaults alone. We assess the readiness of all systems and your entire network, including the status of HIPAA and PCI/DSS compliance, among other regulatory requirements.

Need a hand fortifying and optimizing cyber defenses? Call us for a cybersecurity assessment.

The Logical Advantage

Viewpoint

How a Virtual CIO (vCIO) Drives Strategic Growth

Nearly three-quarters of technology and business professionals rate digital solutions as a primary factor in achieving strategic objectives, according to research by tech trade group CompTIA. Moreover, nearly half (48%) of the executives polled reported their perception of ROI from tech spending is "good" or "excellent."

Where are these leaders applying digital solutions? The top priorities are:

- Enhancing efficiencies
- Building a skilled workforce
- Innovating and cultivating new ideas
- Launching new products and services
- Identifying new customer segments
- Diversifying revenue via new product lines

In other words, senior leadership uses technology mainly to grow business. We believe the same IT best practices that work for large corporations should apply to SMBs.

At a big company, the chief information officer (CIO) refines ways of working with customers, streamlines workflows for greater productivity, contributes to risk management and more. As a top-tier managed services provider (MSP), we can play a similar role as a partner rather than an employee, helping your management team:

- Develop technology roadmaps
- Budget for IT implementations
- Assess cyber risks such as ransomware
- Manage relationships with tech vendors
- Support your leadership with our technical expertise

Think of us as your organization's virtual CIO. Give us a call to discuss our recommendations.

IT Strategy

4 Essential Security Policies

Disruption caused by breaches and the loss of critical data can cripple any company from big enterprises to SMBs.

Case in point: The FBI's Internet Crime Complaint Center received a record 847,376 complaints in 2021, with potential losses exceeding $6.9 billion. Tallies for 2022 have not been released but, given escalating trends, these stats are likely to reach new highs.

How do you protect against financial losses from cybercrime? One solution is employee education. Teach your staff to become the frontline in today's cyberwars. Security policies make great training tools toward this end because they contain the essential information you need to safeguard your organization.

Here are four essential policies that promote IT security education:

- **Acceptable Use Policy**—Also called an AUP, this agreement between employees and the company specifies the appropriate use of access to networks and the internet, clarifying what users may and may not do.
- **Data Breach Response Policy**—This document describes the process followed in the wake of an information security incident, including definitions of a breach and who is involved in the response.
- **Disaster Recovery Plan Policy**—This plan launches when operations must recover from the loss of IT capabilities, whether by natural or virtual catastrophes.
- **Password Protection Policy**—These rules guide creating, using and maintaining strong passwords.

Whether you draft policies yourself or use templates, we can help. Give us a call for a consultation.