The Logical Advantage

TeamLogicIT®
Your Technology Advisor

SEPTEMBER 2023 ISSUE

Technology Trends

Collaborate More, Risk More Cybercrime

Today's work environment involves unprecedented digital collaboration between colleagues, customers and partners. In fact, most organizations work with six or more communication tools, such as email, video conferencing and shared calendaring.

Although these tools can boost productivity, cybersecurity experts contend that increasing communication channels broadens the opportunity for cybercrooks to launch socially engineered technology attacks.

Studies indicate that business email compromise is the most common assault technique for planting ransomware onto networks and other IT systems. Ransomware is particularly vexing for small- to medium-size businesses (SMBs), who are seeing ransom demands increase along with the cost of cybersecurity insurance.

Moreover, paying ransoms does not guarantee data will be released. One survey of ransomware victims who paid ransoms discovered that more than a third of respondents admitted their data was never recovered. And while filing insurance claims remediates some financial damages, the fact remains many firms may lose critical information permanently.

That's why we advocate that SMBs take these preventative steps:

1. Evaluate the scale and scope of your threat landscape regularly.

2. Establish definitions and standards for cybersecurity practices.

3. Identify triggers (e.g., new collaboration platforms) for implementing and/or updating protective measures.

We have walked dozens of clients through this process. Call us for a consultation.

Viewpoint

Rebuff Ransomware with Managed Services

Is digital extortion by ransomware easing or intensifying? The answer depends on the research you read.

While some sources show a slight decrease in ransomware payments over the past 12 months (perhaps because of increased education), others show that individual ransomware attacks have grown more lucrative in recent years. Moreover, data from one cyber insurer reveals both a reduction and rebound trend, as ransomware activity dropped by 25% during the first half of 2022 but swelled by 300% as 2023 began.

As puzzling as these trends may seem, three inconvertible facts clarify the need for action, whether the numbers are up or down:

1. Virtually all companies collect and store sensitive information worth stealing in the eyes of cybercriminals, such as financial data and customer and employee records.

2. Thousands of organizations of all types are assaulted every day around the clock.

3. Nearly three-quarters of all cyberattacks, ransomware or otherwise, that could breach that data are aimed at small to medium-size businesses (SMBs).

That's why as a premier managed services provider (MSP) we recommend SMBs avail themselves of these three tiers of technology support:

Proactive IT — Strategic evaluation and tactical planning provides the flexibility and scalability required to meet market demands and business initiatives.

Preventative IT — Remote monitoring anticipates problems before they occur, preventing disruptions to your operations.

Responsive IT — A local team of highly skilled technicians responds to your needs, both onsite and remotely.

IT Strategy

Communication Key for Disaster Recovery

Research shows nearly 42 million data breaches were detected worldwide during the first quarter of 2023. But while that figure represents a drop of nearly 50% from the fourth quarter of last year, statistics offer little solace to individual companies victimized by breaches.

According to IBM, despite variables such as the extent of an incident, the size of the breached firm or the industry where it operates, the average time from identifying a breach through remediating damages could stretch longer than nine months.

Preparation before data catastrophe strikes can reduce damage to your company's operations, finances and reputation. We encourage clients to create backup and disaster recovery plans (BUDR) with these key characteristics:

- Repeated cyclical assessments of physical and IT vulnerabilities to disasters caused by either cyber or natural forces
- Recurring recalculations of time-to-recovery in response to multiple scenarios
- Regular comprehensive testing of backup procedures and the quality of backed-up data

One factor that can accelerate response and recovery time is communication inside and outside an organization. Here are the essential elements:

- Identify who within your company will communicate with whom and when, not just internally to operations and IT teams but externally to customers, partners and regulatory agencies.
- Write scripts for different disaster scenarios, with blanks to fill depending on the situation.
- Rehearse your communications process just as you would practice other backup routines.

We have extensive BUDR checklists. Call us for help completing yours.

Visit our blog for more trending technology articles at TeamLogicIT.com/blog.