The Logical Advantage

TeamLogicIT®
Your Technology Advisor

OCTOBER 2024

Cybersecure Policy Prioritizes People

Analysts predict that as many as nine of every 10 data breaches this year will involve some form of human error. Recent studies also reveal:

- In some organizations, less than 10% of employees generate 80% of all security incidents.
- Social engineering scams target management 2.5 times more often than other staff.
- Cybercrooks increasingly target small and medium-sized businesses (SMBs) because those firms collectively employ more than 60 million people, nearly half the nation's workforce, representing nearly half all U.S. economic activity.

That's why 20 years ago CISA, the federal agency charged with cyber defense, designated every October Cybersecurity Awareness Month to bolster vigilance across the population "at home and abroad."

But while crucial to deflecting cyberattacks, awareness alone is not enough to mitigate the tremendous risk cybercrime poses. A single data breach can cost a business millions of dollars, perhaps bankrupting an SMB enterprise.

The latest security technology alone is not enough, either. Cybersecurity technology requires good systems grounded in sound policy and disciplined practices, which is why risk managers across industries recommend business leaders prioritize human behavior when designing cybersecurity infrastructure.

As a premier managed services provider (MSP) we believe secure IT requires a computing culture of monitoring and maintenance that expects people, not programming, to make the critical difference.

How? We have protocols and checklists to share. Call us for a consultation.

The Logical Advantage

Viewpoint

Leadership is an SMB's Best Cyber Defense

Recent research illustrates the rising wave of cybercrime against small to medium-sized businesses (SMBs) – eight in 10 ransomware attacks target firms with fewer than 1,000 workers.

That's why as a premier IT managed services provider (MSP), we encourage SMB leaders to incorporate these six National Institute of Standards and Technology (NIST) protocols into their risk management regimen:

1) Identify vulnerable systems.
2) Monitor internal and external threats.
3) Determine probability of incidents, estimate potential impact – tangible and intangible.
4) Analyze controls in place, search for gaps.
5) Calculate likelihood of incursions.
6) Prioritize response and recovery planning.

Extend these principles into IT operations by establishing a bulwark of essential policies:

- **Acceptable Use Policy** for all company devices.
- **Breach Response Policy** with timelines and specific steps.
- **Disaster Recovery Policy** that covers physical and digital incidents.
- **Password Protection Policy** including multifactor authentication measures.

Perhaps the most important cybersecurity initiative SMB management can lead is budgeting. Effective cybersecure computing requires that security safeguards receive full funding annually, anticipating and adjusting for inevitable escalations in threat levels and the costs of coping with them. Call us for additional IT management insights.

IT Strategy

BEC: Your #1 Cybersecurity Threat

Studies show these are the most common techniques enabling cybercrime:

- **Ransomware** – Cybercriminals penetrate company networks, take over servers and encrypt vital operating data. To return access and control, perpetrators demand firms pay ransoms in the form of cryptocurrencies.
- **Data Theft** – Hackers obtain unauthorized access to private systems and steal proprietary information such as user IDs, passwords and other identifiers. These thieves then sell this data to other malefactors through brokers on the dark web, a series of servers containing encrypted content for illicit purposes. How valuable is this stolen info? Estimates run in the billions.
- **Social Engineering** – Cybercrooks deceive individuals into divulging confidential information – typically access credentials. This digital identification then becomes a primary lever for executing the first two digital crimes. Social fraudsters use automation to stage campaigns at immense scale with a broad scope of targets – from frontline workers to C-suite executives.

Each method of cyber scam evolves continually, benefiting from innovations in legitimate technologies such as generative AI. But each also relies on a basic pillar of IT infrastructure: email. Tech researchers speculate that nine of 10 cyber incursions originate via email.

That's why business email compromise (BEC) is your company's prime cybersecurity threat. How do you cope? We have proven policies, practices and protections to share. Call us for a custom consultation.

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

IT inflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor