The Logical Advantage

TeamLogicIT®
Your Technology Advisor

Technology Trends

Align with CISA Cybersecurity Strategy

Earlier this year the Cybersecurity and Infrastructure Agency (CISA) released its strategic plan for 2024 through 2026. The plan focuses on three overarching goals: address immediate threats, harden the terrain and drive security at scale.

Each goal has three underlying objectives:

- **Addressing immediate threats** includes monitoring, mitigating and managing cybercrimes like ransomware, which analysts estimate causes trillions in economic damage annually.
- **Hardening terrain** involves investigating past attacks, planning for future ones and investing in policies and procedures for doing so.
- **Driving security at scale** means supporting a national ecosystem of solutions developers, technical experts and cybersecurity specialists enabled by technology and entrusted with accountability.

We encourage leaders of small to medium-size businesses (SMBs) to develop their own cybersecurity strategies for the coming years. Start with these five assessments:

1. **Risk report** – an executive-level summary with charts, graphs and a vulnerability "score"
2. **Policy review** – includes written documents pertaining to devices, passwords, breaches, remote work and other pivotal areas
3. **Permission report by computer** – a comprehensive list of every device sharing network resources
4. **Permission report by user** – a comprehensive list of every individual with credentials, including level of access
5. **Compliance review** – considers industry and regulatory requirements, identifies risks, gauges exposure and estimates potential fines

The Logical Advantage

Viewpoint

Avoid Breach Losses with Targeted Assessments

Losses from data breaches continue to cost organizations significantly in terms of both financial and reputational damages. Annual cybersecurity research by IBM found that data breach costs have been rising by more than 15% on average over the last three years.

Researchers calculate cost using four areas of financial impact: detection and escalation, notification, post-breach response and lost business

Other findings from IBM's global study:

- The detection and evaluation component of cost spiked nearly 10%.
- The time from initial detection to full recovery stretched to 277 days on average.

While sizeable damages to large multinational corporations drive up the average cost of a breach, the harm is proportional to small to medium-size businesses (SMBs).

How can SMBs avoid contributing to these escalating statistics? We recommend four assessments that evaluate aspects of cybersecurity:

- **Network assessment** – Where are your vulnerabilities along today's ever-spreading perimeter?
- **System assessment** – How thorough is your monitoring and detection of operations that increasingly involve the cloud?
- **HIPAA assessment** – What are your exposures related to this sensitive data, a favorite target for cybercrooks?
- **PCI/DSS assessment** – How comprehensive is your compliance with the Payment Card Industry Data Security Standard?

IT Strategy

Training: Still the Best Cybersecurity Defense

Studies show small to medium-size businesses (SMBs) rely on social media for customer contact and growth. According to SCORE, a research partner of the Small Business Administration (SBA), nearly half of SMB owners cite social media as their preferred means of digital marketing. Moreover, 73% say social channels are their most successful form of digital marketing.

That's why many cybercrooks make social channels—in addition to related channels such as texts, emails and phones—their favorite attack vectors.

Their method involves deceiving users to gain access credentials, which they use to steal proprietary data or lock valuable databases. Then, criminals demand ransom payments and/or sell purloined information through illicit digital marketplaces.

Here are some common "social engineering" techniques used by bad actors:

- An email or text asking receivers to click links to fake websites that capture credentials
- Phone calls asking recipients to call back rather than click a link
- Junk messages, usually delivered by email, that encourage addressees to download attachments that deliver malicious programs such as ransomware

According to the FBI's Internet Crime Complaint Center (IC3), during the last five years most of the more than three million grievances filed involved SMBs.

How can SMB leaders deflect this criminal onslaught? We recommend training as the solution because informed employees are your best defense. Teach staff about policies, protocols and products that insulate your business from cyber-exposures.