The Logical Advantage

TeamLogicIT®
Your Technology Advisor

FEBRUARY 2024

Technology Trends

Risk Management Drives Cybersecurity

In CompTIA's latest State of Cybersecurity report, researchers concluded: Risk management is the driving force behind a successful cybersecurity strategy.

Analysts wrote that, when cybersecurity professionals 1) identify various risks, 2) assign probabilities to cyber incidents, 3) determine potential cost, and 4) propose incident response plans, "The link between cybersecurity spending and desired outcomes gets stronger."

Why? CompTIA's experts theorized that thorough risk analysis extends beyond technical topics to examining policies and processes that may have little to do with a company's IT team. Moreover, leading cybersecurity strategy with risk assessments drives decisions involved in sweeping technology initiatives such as digital transformation (DX).

In short, assessing cyber risk can improve not only IT operations, but performance across an organization. Applying a formal risk management framework can amplify this effect, helping identify areas of concern that may lie outside traditional IT system architecture.

That's why we endorse the Cybersecurity Framework from the National Institute of Standards and Technology (NIST) which structures cybersecurity as a 5-step cycle:

1. Identify – Inventory all digital assets, ensure management procedures are in place and active.

2. Protect – Establish, maintain user access, authentication and privilege control.

3. Detect – Consider support from IT managed services providers (MSPs) versed in the latest attack vectors and monitoring techniques.

4. Respond – Designate personnel to handle incident response, including logging and reporting.

5. Recover – Diligently perform automated backups.

We have broad experience and deep expertise in managing cyber risk. We can help. Call us for a consultation.

The Logical Advantage

Viewpoint

Consider Cloud Computing a Route, not Destination

Analysts expect spending by small to medium-sized businesses (SMBs) on cloud technology to exceed a quarter billion dollars this year.

What types of SMBs will be investing in cloud services? Research by the tech trade group CompTIA reveals top vertical industries as healthcare and an array of professional services companies, such as retail, construction and accounting.

How will SMBs use cloud solutions? CompTIA reports the number one priority is “implementing new systems to enhance efficiencies,” followed closely by “identifying new customer segments / new markets,” then “innovation / cultivating new ideas and putting them into practice.”

Each of those priorities plays a role in profitability by boosting productivity and fostering growth.

That’s why we encourage SMB business leaders to think tactically about operating through the cloud, rather than strategically. Pause a moment, go back and reread that last line.

Now, let’s clarify: Digital transformation (DX) is a strategy, a plan for advancing your business past competitors by applying digital technologies faster and better than they do; cloud computing is a set of digital tactics that support your DX strategy.

Here are examples of tactical cloud applications:

- File synching/sharing
- Backup/recovery routines
- Customer/employee service apps
- Sales/marketing campaign automation
- Secure email platforms

In short, consider the cloud as the route you take, not the place you arrive. Because figuratively many of your virtual operations will travel through the cloud virtually every day.

Give us a call. We’ll help you keep the traffic flowing smoothly.

IT Strategy

Enable Knowledge Workers for Hybrid Work

Small to medium-sized businesses (SMBs) represent an enormous segment of the U.S. economy, providing nearly half of all employment and contributing about half of all dollars spent on tech.

Per McKinsey, as a collective sector SMBs outspend large enterprises in some technology segments. And soon, one category that could reach that level is communication and collaboration systems.

Why? Two driving factors:

1. An escalating trend toward hybrid working

2. The types of workers doing that kind of work.

A recent Gartner study predicts this year more than half our nation’s “knowledge workers” will be hybrid workers.

Who is a knowledge worker? In basic terms, any staffer accumulating business knowledge and then applying that expertise to serve clients and drive operations. Because many SMBs populate vertical industries such as healthcare and financial services, many of those SMBs have a high population of knowledge workers. And those workers increasingly need hybrid IT for communication and collaboration.

How can you support these workers? We advise focusing on three areas:

- **Readiness**—Working from anywhere at any time requires a combination of hardware, software and connectivity solutions.
- **Policies**— Hybrid work necessitates a combo of business policies, too, for acceptable use of equipment and networks, cybersecurity protocols, and disaster response and recovery.
- **Security**—Likewise, stable hybrid IT demands secure measures such as multi-factor authentication (MFA), VPNs and continuous monitoring.

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

IT inflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT® Your Technology Advisor