The Logical Advantage

TeamLogicIT® Your Technology Advisor

NOVEMBER 2023 ISSUE

Technology Trends

Ransomware Threatens Business Continuity

Analysts at cryptocurrency research firm Chainalysis say crooks perpetrating ransomware schemes are on pace for their second most lucrative year in cybercrime history.

But the immediate damage from ransoms isn't the only financial threat posed by ransomware. Researchers from the cloud security firm BigID discovered that 67% of executives polled "lack full confidence their company could recover data and critical business processes in the event of a systemwide cyberattack."

When asked how long, on average, recovery would take:

- 95% said 24 hours
- 71% said 4 days
- 41% said more than a week

Post ransomware incursion, every minute matters. The longer data is inaccessible, the greater the business risk. That's what makes these findings troubling for small to medium-size businesses (SMBs) as they often lack the budget, experience and in-house technical skills for effective business continuity planning (BCP.)

One way to mitigate ransomware's risks to your business continuity is a data backup and recovery routine. These are the basic components of such a routine:

A. **Local image** – continual backup for your operating system, applications and databases

B. **Offsite backup** – nightly backups by cloud-server virtualization, preserving data in the event of physical or digital disasters

C. **Hybrid services** – a combination of local and offsite backups, enabling restoration from remote locations

We have helped thousands of businesses develop BCPs that minimize losses and accelerate recovery. Give us a call for help with yours.

Viewpoint

Hybrid Work Makes Cloud Tech Critical

Recent research revealed an unexpected group of employees pushing for hybrid working models in the post-pandemic era: Senior executives.

Nearly half the high-level staffers polled by management consulting firm McKinsey said they were likely to quit their jobs if required to return to the office every weekday. The same group reported they were willing to trade more than 20% of their compensation to work their desired number of days from home.

The preferences of senior leadership can sway company culture at any size organization. But these tendencies are especially influential at small to medium-size businesses (SMBs), where staff retention is critical to productivity and profitability.

That's why investing in cloud computing is more important than ever for SMBs. Not only do secure, flexible, scalable cloud services enable your team to work anywhere at any time, these transformational virtual solutions empower small organizations to compete with larger and better-funded competitors.

Key advantages of cloud technologies include:

- **Flexibility:** Access files using web-enabled devices such as smartphones, tablets and laptops, allowing teams to collaborate and share documents and other data via internal or external internet connections.
- **Scalability:** Add "seats" and additional features when headcount rises and/or business requirements change; do the inverse if staffing is reduced or economic conditions tighten.
- **Cost-effectiveness:** The "as-a-service" consumption model means pay as you go, with smaller periodic payments (e.g., monthly, annually) rather than acquiring costly software and servers.

The cloud offers many more business benefits. Please reach out if you'd like to discuss its potential advantages for your company.

IT Strategy

ABCs of BEC (Business Email Compromise)

Business email compromise (BEC) is a cybercrime involving fake messages designed to trick receivers into divulging confidential company information. Crooks pose as trusted colleagues or associates and then ask recipients to pay false bills or provide credentials for access to proprietary data.

But BEC scammers do not limit their attacks to email. Studies show these cyber thieves use text messages about 30% of the time, social media connections for another 30% of attacks and phone calls for about 20% of intrusions.

Faux links are often the tactic used to capture sensitive information. In fact, most data breaches start with one person clicking a seemingly safe link.

Typical BEC scams include:

- **Data theft** – First, BEC criminals steal company information from financial reports, an HR database or similar sources. Next, they include facts from these records to make fake messages feel authentic.
- **C-suite spoofing** – Cybercrooks hack C-level email, and then direct staffers to pay invoices, make purchases or authorize other spending. They often use falsified attachments that may feature bogus account numbers or appropriated logos from well-known banks to appear legitimate.
- **Advisor spoofing** – This social engineering technique applies the same mechanism as C-suite spoofing. But instead of impersonating authorities inside the company, perpetrators mimic advisors outside the organization—e.g., accountants, lawyers, even IT help desks.

The FBI recommends user education as a best practice for thwarting BEC. As part of our managed services, we offer cybersecurity awareness programs. Let us know if this is an area where you need assistance.

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

ITinflections NAVIGATING TECHNOLOGY FOR BUSINESS®

TeamLogicIT®
Your Technology Advisor