THE LTO PROGRAM
Security Survey Findings
June 2021
In June 2021, The LTO Program conducted a unique data security survey with more than 120 IT executives to find out what their fundamental security concerns are and what actions they are taking to defend against cyber-criminal activity. Key findings include:

- **Ransomware/Cybersecurity is a top concern for organizations.** Over 35% of respondents ranked ransomware/cybersecurity as their top data storage concern.

- **Organizations are experiencing an increase in cybersecurity attempts.** For those who listed ransomware as a top concern, more than half indicated that they’re seeing an increase in attempts. Interestingly, nearly 40% said that remote access during pandemic was another driver.

- **Different systems are used to mitigate ransomware risk.** For those who didn’t list ransomware as a top concern, more than half have systems in place to mitigate risks, such as offline storage.

- **Offline data backup is important in protecting data.** The policy/measure that is most important in protecting data from ransomware is offline data backup – overwhelmingly at more than 80%. Employee education was a close second.

- **Restoring from offline backup is critical.** If systems were attacked by ransomware, 7 in 10 surveyed would restore from an offline backup. Only 15% cited cloud.
RANSOMWARE/CYBERSECURITY IS THE TOP DATA CONCERN IN 2021

Ransomware + Cyber Security 36%

Exponential Data Growth 25%

Budgets 22%

Data Migration 14%

QQ: What is your top data concern in 2021?

*Other top data storage concerns for organizations include: backward compatibility, interoperability, backup speeds, cost of tape media, cartridge longevity
We have systems in place to mitigate risks such as: object lock; offline storage; other vault-like solutions 59%

We have not faced any ransomware attack in the past 29%

It’s not something that my department manages 22%

Ransomware doesn’t impact our environment 13%

We have insurance in place to cover for any ransomware incidents 7%

Other 12%

QQ: If ransomware/cybersecurity was NOT listed among your top concerns, what are the reasons why? (N=91)
OVER HALF OF RESPONDENTS ARE SEEING AN INCREASE IN RANSOMWARE ATTACKS OVER THE PAST YEAR

We’re seeing an increase in ransomware attacks over the past year: 51%

We do not want to risk loss of revenue or reputation: 40%

Amid the pandemic, we’ve had to support more remote access for employees/challenge of more access from outside firewall: 39%

We do not want to risk loss of revenue or reputation: 27%

Ransomware/security was not listed among my top concerns: 24%

QQ: If ransomware/cybersecurity was listed among your top concerns, what are the reasons why?

*N=117*
OFFLINE DATA BACKUP IS MOST IMPORTANT TO ORGANIZATIONS IN PROTECTING FROM THE IMPACT OF RANSOMWARE ATTACKS

QQ: Which policy/measure do you feel is most important in protecting your organization from the impact of a ransomware attack?

*Other policy/measures include: Isolated data networks, Intrusion detection, Parallel tracking systems, Personal integrity, 3-2-1 backups, IPS/IDS/SIEM LAN segmentation with NGFW, and Proper security systems with enterprise firewalls
ABOUT 1 IN 3 ORGANIZATIONS SAW AN INCREASE IN ATTEMPTED RANSOMWARE ATTACKS IN 2020

Yes 37%
No 32%
Not sure 31%

QQ: Did your organization see an increase in attempted ransomware attacks in 2020?
OVER 60% OF DATA MANAGERS ARE SEEING A 1-25% INCREASE IN ATTEMPTED RANSOMWARE ATTACKS

QQ: If you did see an increase in attempted ransomware attacks in 2020, how large of an increase would you estimate that to be?

*N=91
56% of organizations are experiencing ransomware attacks at least 2-3 times per year.

QQ: What is the typical frequency of ransomware attacks that you face?
70% OF ORGANIZATIONS WOULD RESTORE DATA FROM OFFLINE BACKUP IF IMPACTED BY A RANSOMWARE ATTACK

- **70%** Restore data from offline backup/tape/NAS/Object lock
- **15%** Restore data from cloud/remote backup
- **6%** Contact authorities
- **7%** Work with insurance company/external consultants to recover/negotiate with attacker to obtain encryption key
- **2%** Other*

*Other implementation actions for organizations include: Isolate the attack, restore data from parallel tracking system, contact authorities

QQ: If your system were to be impacted by a ransomware attack that locked out access to critical data, what would be the actions that you’d implement?
**RESPONDENT PROFILE**

**Industry of Organization**

- **Media & Entertainment**: 37%
- **Technology or Cloud Service Provider**: 21%
- **Manufacturing**: 7%
- **Government**: 6%
- **Healthcare**: 6%
- **Finance**: 1%
- **Other**: 21%

*Other industries of organizations include: Education, Retail IT Support, Non-profit, Agriculture, Transport/Travel, and Research*

**TBs of Data Managed**

- **51 TB - 200 TB**: 24%
- **Less than 50 TB**: 22%
- **1 PB - 5 PB**: 22%
- **More than 5 PB**: 21%
- **21 TB - 150 TB**: 11%