EGNYTE

Cybersecurity Trends for Mid-Sized Organizations

Data Governance Trends Report Mid-Year Update

July 2022

Methodology

The data appearing in this report was collected by an independent research firm, which surveyed 400 US C-Level executives, at companies of 100 to 1,000 employees. Utilizing an e-mail invitation and an online survey, the survey was conducted in May 2022.

Key demographic details about respondents include the following:

- **53%** work in CIO, CTO or IT Security roles. Another **18%** work in data-related roles.
- **33%** have been at their organizations for 10 years or more.
- **48%** of their organizations employ fewer than 499 people, while **52%** of their organizations employ more than 500 people.
- **58%** of their organizations generate less than $100 million in revenue, while **42%** generate more than $100 million in revenue.
- **54%** of their organizations have been in business for more than 15 years, and **46%** of respondents' organizations have been in business for more than 15 years.

Summary Findings

1. **Companies Still Battle with Data Sprawl**
   51% of respondents' organizations manage more than 10 data repositories.
2. **Data Backup & Recovery Rates are Promising**
   58% of respondents' organizations test data backup and recovery processes for critical data on a daily basis.
3. **Cybersecurity Training's Become a Bigger Focus**
   63% of respondents' organizations conduct cybersecurity training on at least a quarterly basis.
4. **Cyber Insurance Premiums are Skyrocketing**
   47% of respondent's organizations have experienced premium increases of 76% or more in the past year.
5. **Formal Incident Response Plans Aren't Prevalent Enough**
   Only 64% of organizations have a formal incident response plan in place.
6. **Administrative Controls Can be Lax**
   31% of respondents' organizations permit users to add other users to repositories that store sensitive data, without IT's involvement.

Detailed Findings:

1. Pricing for **cyber insurance** premiums continues to increase rapidly. However, most organizations are confident that their cyber insurance claims will ultimately be paid.

Cyber Insurance

- On a positive note, 100% of respondents' organizations purchase cybersecurity insurance.
- 90% of respondents' organizations have experienced cyber insurance premium increases in the past year.
- 73% of respondents' organizations are completely or mostly confident that potential claims for cybersecurity incidents - such as malware or breaches that are perpetrated through supply-chain partners - will be paid.

2. Fewer than 50% of organizations train more than 75% of their employees in **cybersecurity awareness**. For companies that prioritize training, it's clear that a "once a year and done" strategy isn't sufficient: Only 6% of companies train their employees annually.

Cybersecurity Awareness Training

- Only **38%** of respondents' organizations require 75% to 100% of their employees to be trained or certified in cybersecurity awareness.
- The average percentage of respondents' employees who are required to be trained or certified in cybersecurity awareness is only **61%.**
- In a promising sign, **63%** of respondents' organizations conduct cybersecurity awareness training at least once a quarter.
- Disappointingly, only **58%** of respondents' organizations provide ongoing education about the potential link between suspicious e-mails and ransomware attacks.

3. **Data sprawl -** which can increase potential cyber-attack surface and impact users' business productivity - continues to be widespread.

Data Sprawl

- **86%** of respondents' organizations manage between 6 and 15 data repositories.
- **51%** of organizations manage more than 10 data repositories.
- **66%** of respondents' organizations evaluate their data management infrastructure at least once a quarter, to detect potential "Shadow IT" repositories.

4. Nearly three-fifths of organizations test their **data backup & recovery** processes for critical data on a daily basis. Conversely, nearly 15% of organizations test for critical data once a week or less, which can create a conducive environment for cyber-attackers.

Data Backup & Recovery

- **All** of the respondents' organizations had defined data backup & recovery policies in place.
- **43%** of respondents' organizations test their data backup & recovery processes for critical data less than once per day.
- **14%** of respondents' organizations test data backup & recovery processes for critical data less than once a week.

5. Most mid-sized organizations have implemented basic **cybersecurity hygiene** practices, including putting processes in place to report cybersecurity incidents and utilization of Endpoint Detection & Response (EDR) and Multi-Factor Authentication (MFA).

Cybersecurity Hygiene

- **100%** of respondents' organizations have a reporting mechanism in place for potential cybersecurity incidents.
- **89%** of respondent's organizations mandate MFA for access to all services.
- **75%** of respondents' organizations utilize an EDR solution.
- **66%** of respondents' organizations have formalized plans in place to report potential incidents, and **61%** of organizations have data purge policies in place.

6. Most mid-sized organizations have technology in place to identify potential **ransomware and e-mail phishing** attempts.

Phishing & Ransomware Detection

- **100%** of organizations report they have processes in place to help identify e-mails that might launch potential ransomware.
- **91%** of respondents' organizations state that they utilize technology which provides automated recovery from ransomware attacks.
- **64%** of respondents' organizations flag e-mails from outside senders; 64% of organizations flag e-mail for malicious domains and 63% utilize e-mail phishing detection technology.

7. A majority of companies track **unusual data access** on their networks, including geographical and/or time of day access.

Unusual Data Access

- **100%** of respondents' organizations have processes in place to detect unusual user access.
- **61%** of respondents' organizations track unusual access to their data repositories by geographical location.
- **59%** of respondents' organizations flag unusual user access immediately.
- **57%** of respondents' organizations have formal processes in place with their IT teams to detect unexpected file or folder access.
- **53%** of respondents' organizations track unusual time of day access.

8. Most organizations require IT administrators to review requests to add users to data repositories that store **sensitive information.**

Users' Access to Sensitive Data

- **69%** of respondents' organizations require IT administrators to review user additions to their data repositories that contain sensitive data.
- **31%** of respondents' organizations permit users to add other users to data repositories that store sensitive content, without IT's involvement.

Implications and Recommendations

01 | Update Your Incident Response Plan

According to published reports, recovery from ransomware attacks took an average of 20 days in Q4 2021. You need to have a plan in place with your technology providers and your legal counsel to reacover rapidly, should a cyber-attack occur. If it hasn't been updated recently, it's one of the best places to start.

02 | Implement an Effective Ransomware Plan

To prevent extended downtime as a result of ransomware attacks and insider threats, snapshot recovery is an effective way to recover files quickly and maintain users' productivity. Consider integrating snapshot recovery with table-top exercises to analyze the effectiveness of your company's business recovery program.

03 | Prioritize Cybersecurity Awareness Training

One of the easiest and least expensive ways to prevent cyber-attacks is to prioritize cybersecurity awareness training. White-hat phishing programs are a great place to start, but only 58% of the study's respondents engaged in them. Make training sessions fun to maximize attendee recall, while encouraging attendees to be candid about required areas of improvement.

04 | Adopt EDR & MFA Solutions

Organizations that don't utilize EDR or MFA solutions are at the highest risk of potential cyber-attacks. And, recent reports show that users who enable MFA on their accounts can block up to 99.99% of automated cyber-attack attempts. By enhancing network security and preventing malicious access to users' accounts, your organization will be better positioned to prevent potential attacks.

Take the Next Step

A key component of cybersecurity success is to work with a trusted partner that has deep experience in the space.

To protect your company from potential cyber-attacks , you should consider technological solutions like the following to bolster cybersecurity protection:

- Data Backup & Recovery
- Restricting Access to Sensitive Data, Based on Users' "Business Need to Know"
- Ransomware Detection & Snapshot Recovery
- Insider Threat Protection & Suspicious Log-In Detection

Your partner should know your industry well and be knowledgeable about rapidly-changing data privacy and cybersecurity regulations.

Find out how solutions like these can benefit you, by watching the Data Governance product tour at the link below.

Take the Tour

EGNYTE

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs. For more information, visit **www.egnyte.com.**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com