Humans Are the Weakest Link

Microsoft 365 Security and Data Breach Headaches

Of IT leaders, **67%** report an increase in data breaches due to remote work versus **32%** whose organizations aren't using Microsoft 365.[1]

IT Leader

Remote employees were almost **twice** as likely to accidentally leak data by **email.**[1]

85% of employees are sending more emails [1]

80% say email is their preferred channel for sharing sensitive data [2]

More emails = more risk. **73%** of employees say they feel more tired, stressed and under greater pressure with remote work [2]

77% of IT leaders believe mobile devices are more likely to leak data than a desktop [2]

This is a clear problem, with **95%** of IT leaders saying that client and company data is at risk on **email** [2]

The three types of **malicious** emails: [4]

- **Phishing:** Trick an individual into sharing sensitive information like usernames and passwords
- **Malware Delivery:** Use either links or attachments to deliver malware
- **Business Email Compromise:** Attackers pretend to be a legitimate business account

61% of IT leaders say clients are frustrated and are asking whether organizations they work with have an email data loss prevention (DLP) in place. [2]

Most Targeted Sectors. [4]

1%	Energy
1%	Health
1%	Media
2%	IT
3%	IGOs
10%	Other
31%	NGOs & Think Tank
48%	Government

Traditional DLP tools. The root of the problem?

Microsoft 365's native email DLP functionality uses static rules, which may not be enough to mitigate all email data loss incidents.

Side Note

There are currently **200,000,000** million active Microsoft 365 users.[2]

43% said they require a high level of admin to maintain [2]

26% said they create user friction [2]

38% of IT leaders downgraded their rules to make them more workable [2]

100% of IT leaders are frustrated by current traditional static DLP rules. [1]

92% The risk is great with **92%** of organizations experiencing negative impacts due to email data breach. [2]

42% said half of all incidents won't be detected by their static DLP tools. [1]

Consequences of a 365 data breach. [3]

- Disruption of Business
- Loss of Intellectual Property
- Reputation Damage
- Legal Ramifications
- Revenue Loss
- Customer Attrition
- Data Loss
- Continued Attacks

83% This happens more often than we think. Over the last 12 months, **83%** of organizations reported their data had been put at risk with email. [2]

Costs:

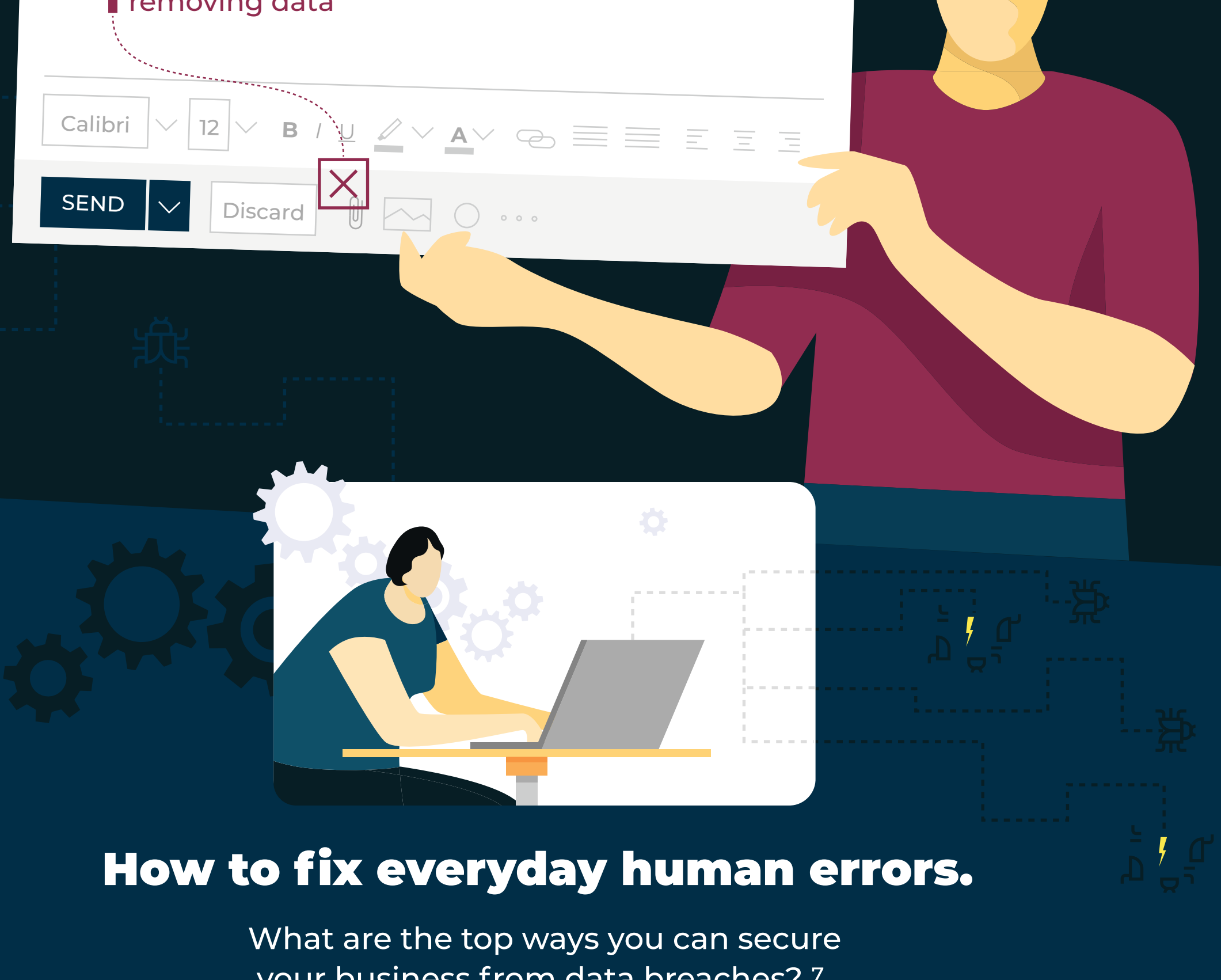
$3.86 Million (2020) — $4.35 Million (2022)

From 2020 to 2022, the average cost of data breaches increased **12.7%** from **$3.86 million** to **$4.35 million.**[5]

For healthcare, a data breach on average can cost **$7.13** Million [6]

Everyday human errors.

Microsoft 365 static DLP rules see a majority of email data breaches from everyday human errors like: [2]



How to fix everyday human errors.

What are the top ways you can secure your business from data breaches? [7]

- Use multi-factor authentication
- Protect admin accounts
- User preset security policies
- Use email securely
- Protect all devices
- Work together in Microsoft Teams
- Set file sharing settings
- Use Microsoft 365 apps
- Manage calendar sharing
- Maintain your environment

How secure are you? Be sure to take the proper steps to ensure your company doesn't get involved with a data breach.

PROSPERSPARK

WWW.PROSPERSPARK.COM

1. https://www.egress.com/blog/data-loss-prevention/microsoft-email-dlp
2. https://www.egress.com/media/n0wi0s0q/egress-2021-data-loss-prevention-report
3. https://onestopit.com/articles/consequences-of-a-microsoft-365-security-breach/
4. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
5. https://www.ibm.com/security/data-breach
6. https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year
7. https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/secure-your-business-data?view=o365-worldwide