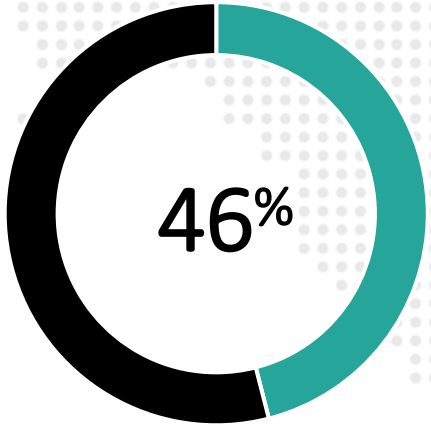
REQUIRED SECURITY CONTROLS FOR REMOTE ACCESS

Ensuring Security Controls Are In Place & Compliant When Utilizing Decentralized IT Environments & A Remote Employee Workforce

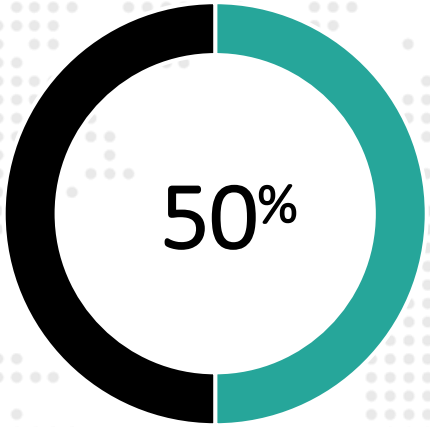
RESTECH SOLUTIONS

REMOTE USERS FACE INCREASING THREATS



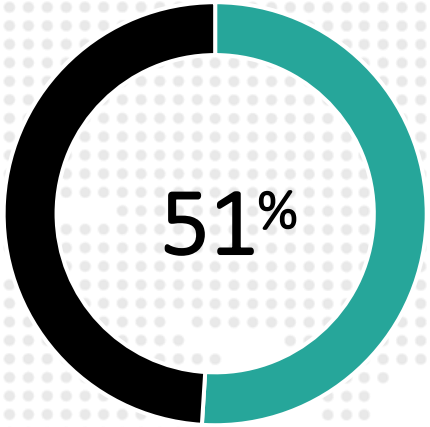
46%

of global businesses have encountered at least one cybersecurity scare post shifting to remote working during the pandemic.



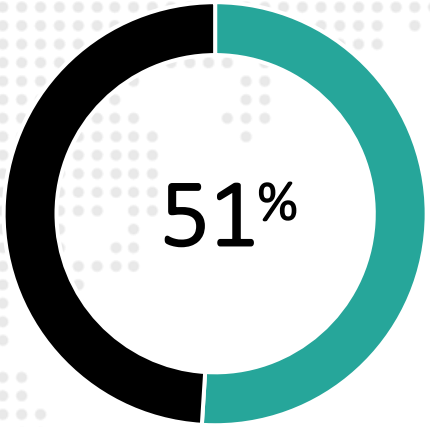
50%

of businesses have allowed employees to use personal email IDs and personal devices to conduct company work.



51%

of businesses have already witnessed an increase in email phishing attacks since the shift to a remote working model.



51%

admitted their workforce isn't proficient or properly trained on the cybersecurity risks associated with remote working.

RESTECH SOLUTIONS

RESTECH SOLUTIONS

43.81%
PHISHING
(compromised credentials)

30.48%
COMPROMISED OR STOLEN CREDENTIALS
(method unknown)

4.76%
BRUTE-FORCE ATTACK
(compromised credentials)

8.57%
RANSOMWARE

8.57%
HACKING

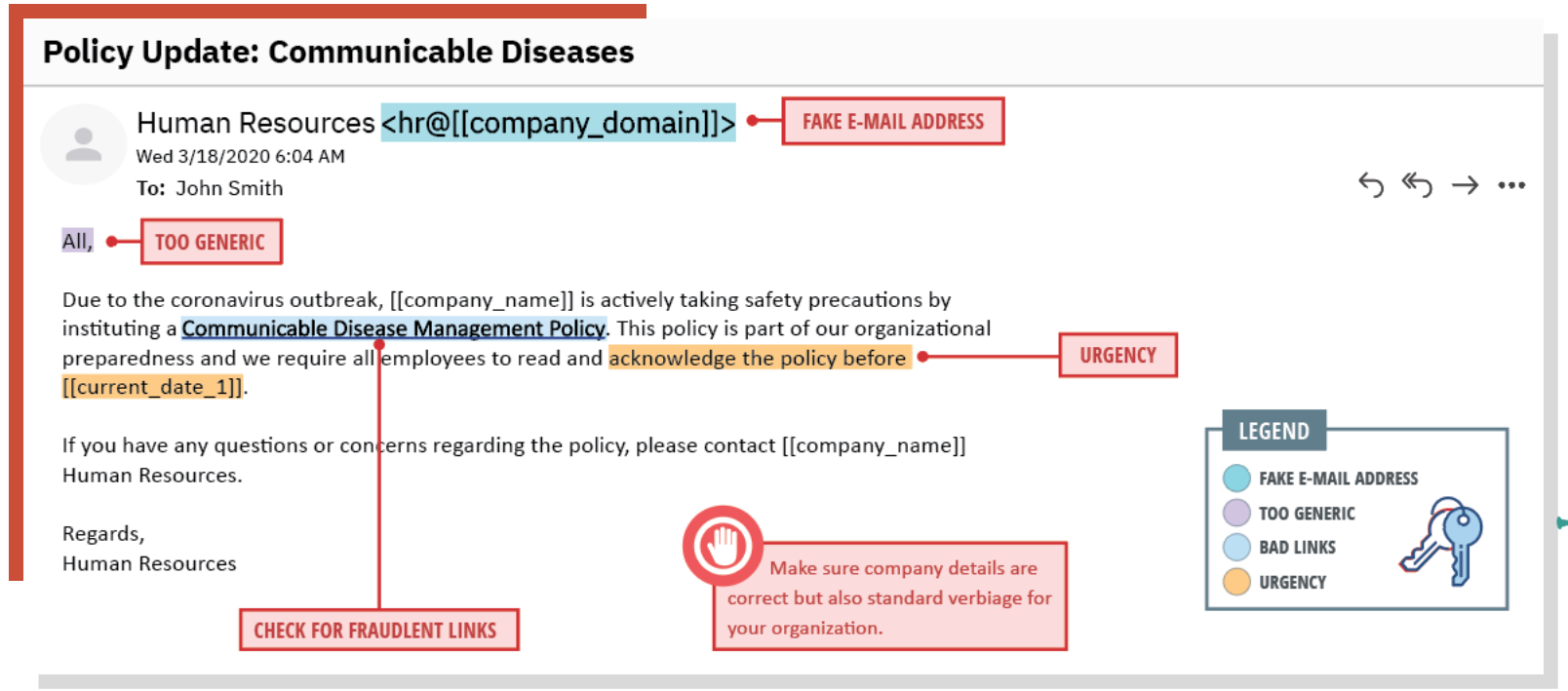
2.86%
MALWARE

0.95%
OTHER

HOW ARE ALL THESE BREACHES HAPPENING?

PHISHING ATTACKS ARE SURGING!

COVID-19 Examples



RESTECH SOLUTIONS

Growing List of Compliance Regulations:

RESTECH SOLUTIONS

DATA PROTECTION

Confidentiality

Integrity

Availability

RESTECH SOLUTIONS

HOW SECURE IS YOUR REMOTE WORKFORCE?

Risk Assessment & Ongoing Monitoring?

Secure VPN Access to Internal Network & Applications?

Personal / BYOD Allowed?

Regular Security Awareness Training?

RESTECH SOLUTIONS

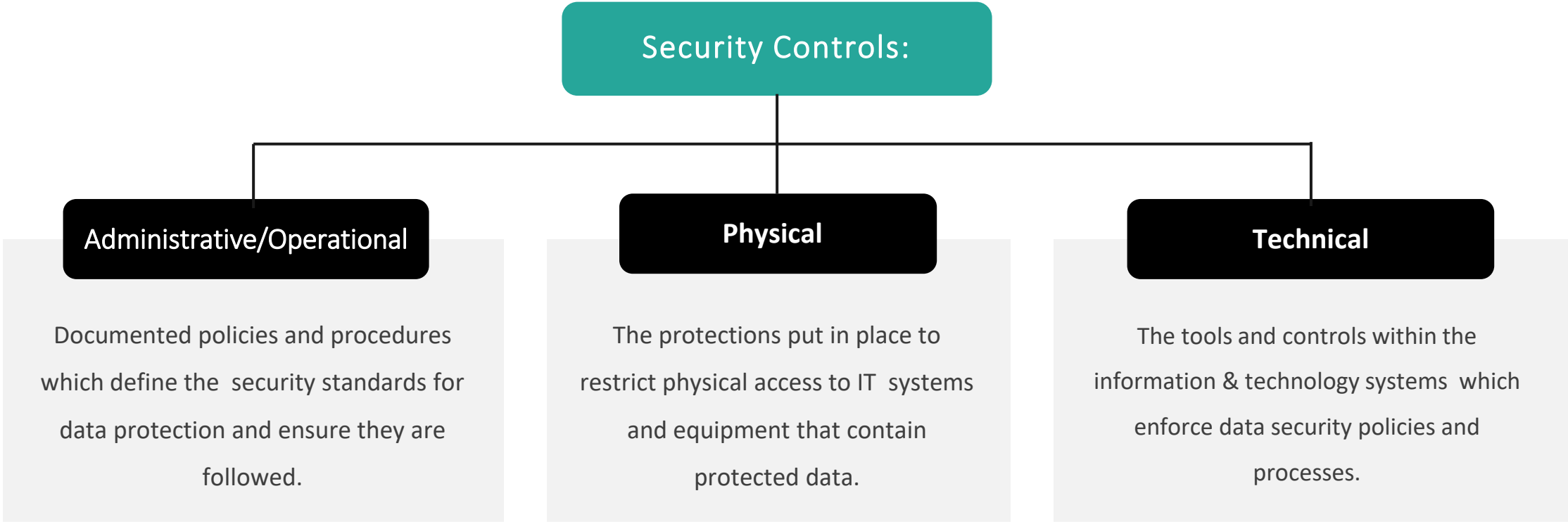
WHAT ARE SECURITY CONTROLS?

The policies, procedures, technology systems and tools, and the physical measures implemented to protect your organization's data and information assets and to prevent or reduce incidents of:

- Unauthorized Access & Exposure
- Accidental Loss or Destruction
- Disruption & Downtime

RESTECH SOLUTIONS

REQUIREMENTS FOR REMOTE ACCESS



RESTECH SOLUTIONS

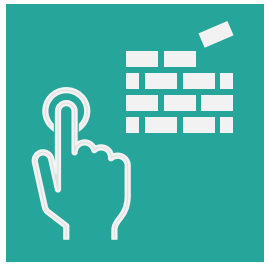
ADMINISTRATIVE OR OPERATIONAL CONTROLS

These may include:

- **Security Management Process**
  Aimed at identifying and analyzing potential risks to all types of sensitive data and implementing security measures to reduce vulnerabilities to an appropriate level.
- **Dedicated Personnel**
  A designated security official or a team charged with developing and implementing security policies and procedures.
- **Information Access Management**
  Managing and limiting access to sensitive data based on the need and a given user's role.
- **Workforce Training and Management**
  Training the entire workforce regarding the security policies and procedures and holding them accountable if they fail to uphold the rules.
- **Evaluation**
  A periodic assessment of how well do a business' security policies and procedures meet the requirements of a regulation.

RESTECH SOLUTIONS

PHYSICAL SECURITY CONTROLS



Facility safeguards such as fencing, guarded gates, or RFID and scanners/readers restricting access.

Facility-Level Access

Locked Rooms or Encasements

Dedicated rooms and cabinets or external casings or housings which are locked to block access.

RESTECH SOLUTIONS

– TECHNICAL CONTROLS

These may include:

- **Identity and Access Management**

  Implementing technical policies and procedures that allow only authorized persons to access sensitive data.

- **Audit Controls**

  Putting in place hardware, software, and/or procedural mechanisms to manage access and activity on devices used for working with sensitive data.

- **Integrity Controls**

  Ensuring that sensitive data is not improperly altered or destroyed.

- **Secured Transmission**

  Preventing unauthorized access to sensitive data while it is being transmitted over a network.

RESTECH SOLUTIONS

PARTNER WITH SPECIALISTS

Detect

Detect your data protection needs as per the regulations you must comply with.

Identify

Identify appropriate measures you must undertake and issues you must address immediately.

Secure

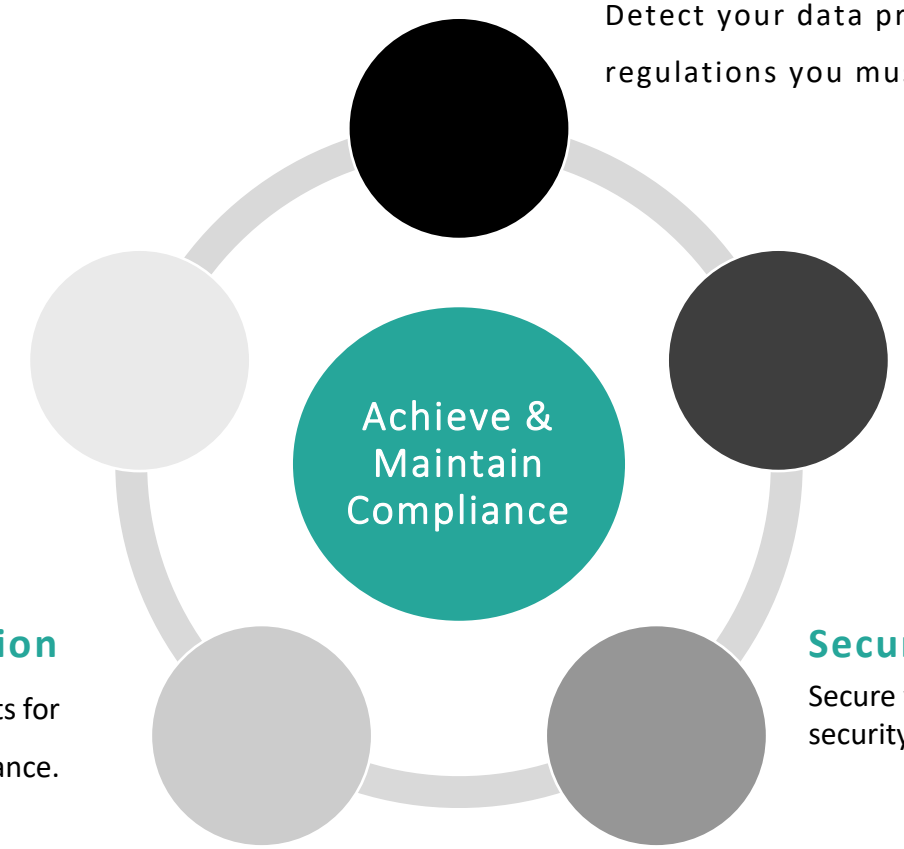
Secure your business with the right data security tools and controls and manage them.

Generate Documentation

Generate mandatory documentation & reports for demonstrating proof of due diligence for compliance.

Provide Support & Guidance

Provide you with the technical support and guidance you need to manage your data protection requirements.



RESTECH SOLUTIONS

KEY SECURITY CONTROLS FOR COMPLIANCE

1 Setup A Secure VPN

Configure a secure VPN or Virtual Private Network for remote users to access the company network systems and data.

2 Secure Home Wireless Connections

Make sure home users have secure home wireless connections that are password protected and encrypted.

3 Encrypt & Secure All Devices

All devices (company-owned and personal) accessing sensitive data must be encrypted and password protected.

4 Automatic Timeouts & Lock Screens

Configure all devices and applications with automated log off timers and screen lock settings.

5 Require 2FA/MFA Access Management

Control who is accessing your network and company data by requiring two-factor or multi-factor identity authentication.

6 Prohibit Credential & Device Sharing

Enforce strict policies and procedures that prohibit or restrict users from sharing credentials or devices with colleagues, family or friends.

7 Implement Email Encryption Tools

Restrict and limit process of *sending sensitive data via emails when possible, otherwise require encryption.*

8 Educate & Train Employees Frequently

Remote users are stressed and overwhelmed and facing increased cyberattacks. It is critical you empower them with frequent security awareness training.

RESTECH SOLUTIONS

RESTECH
SOLUTIONS

THANK YOU