bis

THE ULTIMATE GUIDE

FOR ENGINEERING & ARCHITECTURE FIRMS

on Preventing Costly Data Loss

Ensure you can easily and affordably recover your files with our 8-step data loss prevention strategy

According to Clutch, 60% of small to mid-size organizations that experience data loss will go out of business within 6 months.

TOP 4 CAUSES OF DATA LOSS

Hardware Failure	Natural Disaster
X	⚠

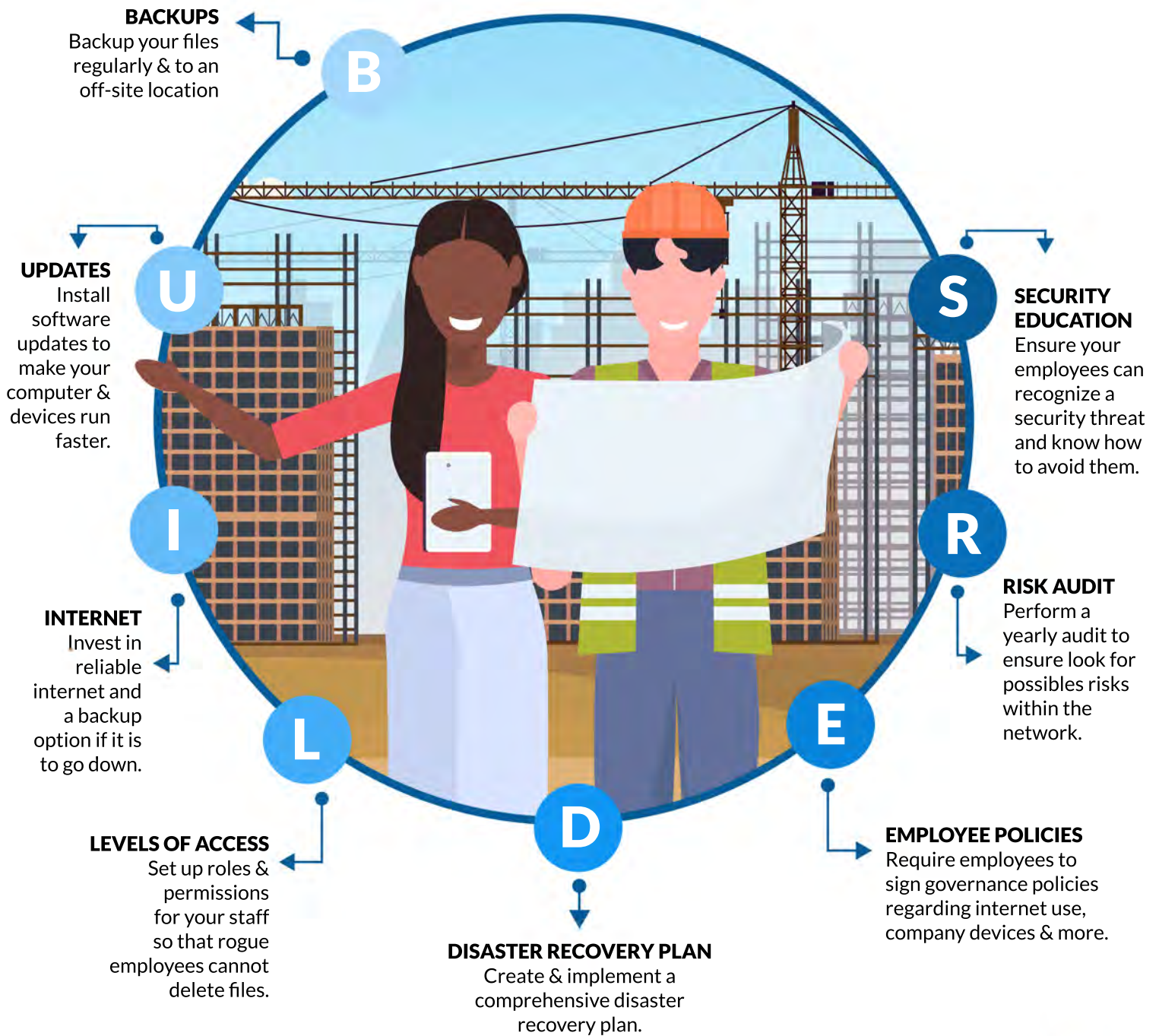| Human Error	Virus
	🐞

The Cause of Data Loss

Since the threat landscape is growing more complex, it leaves firms vulnerable to data loss in more than one way. While rogue employees and natural disasters still pose a threat, firms are now being targeted more and more through ransomware, viruses and other cyber attacks that all lead to data loss. Not to mention, the growing number of lost or stolen mobile devices with non-encrypted company information.

Today, data loss can happen at any time and in any way. The only successful method to protect your firm is with a comprehensive data loss prevention strategy.

Types of Data Loss

THE **BUILDERS** METHOD

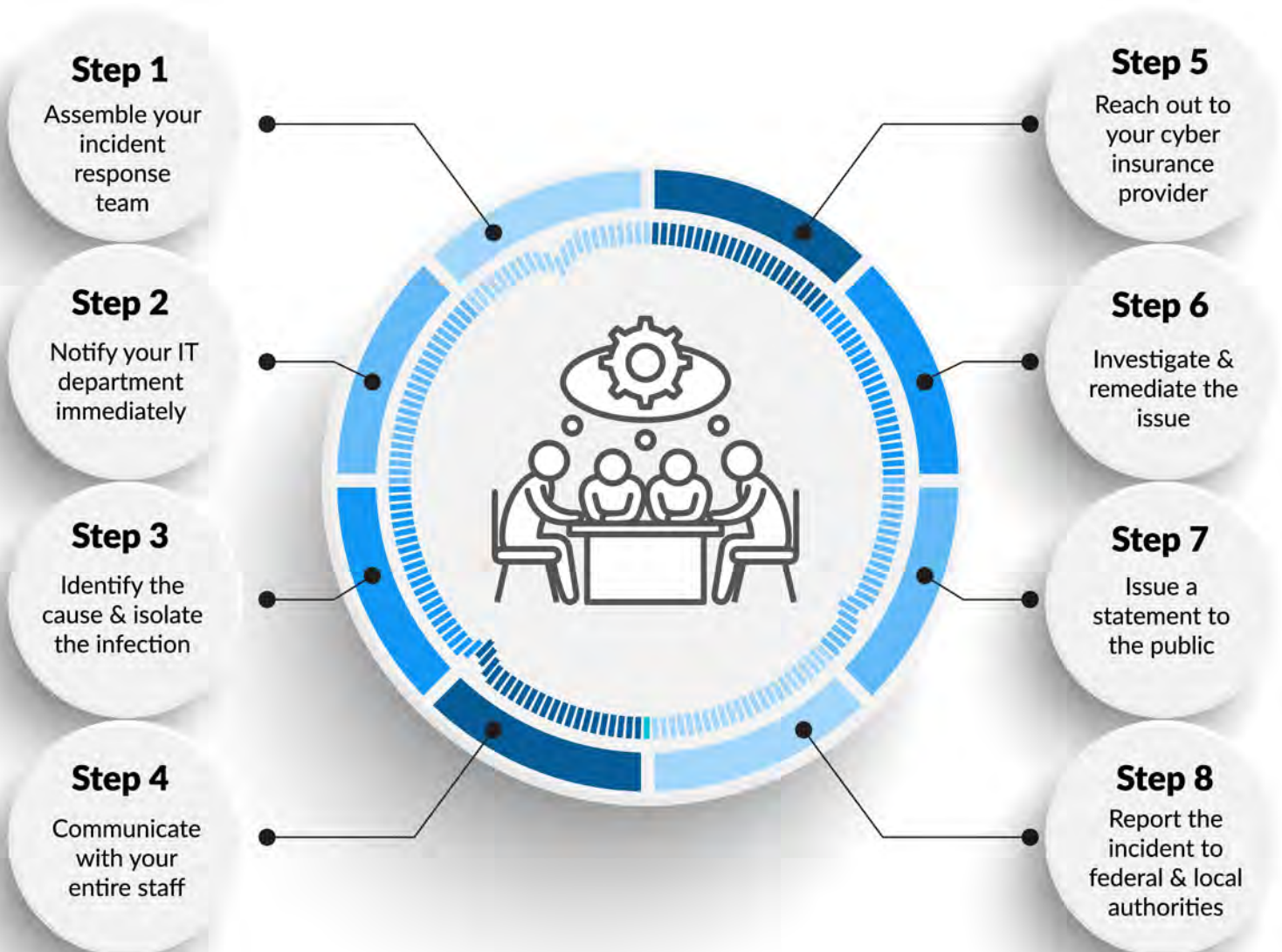Use the BUILDERS Method to prevent costly downtime and data loss.

BACKUPS
Backup your files regularly & to an off-site location

B

UPDATES
Install software updates to make your computer & devices run faster.

U

S

SECURITY EDUCATION
Ensure your employees can recognize a security threat and know how to avoid them.

I

R

INTERNET
Invest in reliable internet and a backup option if it is to go down.

RISK AUDIT
Perform a yearly audit to ensure look for possibles risks within the network.

E

L

D

LEVELS OF ACCESS
Set up roles & permissions for your staff so that rogue employees cannot delete files.

EMPLOYEE POLICIES
Require employees to sign governance policies regarding internet use, company devices & more.

DISASTER RECOVERY PLAN
Create & implement a comprehensive disaster recovery plan.

bis
BUSINESS INFORMATION SOLUTIONS
We Get *IT* Done!

WHAT TO DO ONCE YOU'VE BEEN BREACHED

bis
BUSINESS INFORMATION SOLUTIONS

Getting IT done.

Even after you've implemented the proper security protections, there's still a chance of getting breached. Luckily, your comprehensive data loss prevention strategy should minimize the impact and keep interruptions to a minimum.

Here are the steps you should immediately take upon learning of a security incident or breach:

Step 1
Assemble your incident response team

Step 2
Notify your IT department immediately

Step 3
Identify the cause & isolate the infection

Step 4
Communicate with your entire staff

Step 5
Reach out to your cyber insurance provider

Step 6
Investigate & remediate the issue

Step 7
Issue a statement to the public

Step 8
Report the incident to federal & local authorities

You can report a cybersecurity incident to the Department of Homeland Security by visiting: https://www.us-cert.gov/forms/report

PREVENT COSTLY DATA LOSS

My name is Phillip Long and I'm the CEO of Business Information Solutions. As a cybersecurity and technology specialist, I continue to see engineering and architecture firms who are blindsided by unexpected downtime or data loss which could cost thousands to recover.

It's my duty to help as many firms as possible develop a successful disaster recovery plan and protect themselves from cyber threats so that they can focus on their clients' projects instead of being concerned about downtime.

Phillip Long,
CEO & CISSP

{FREE} CYBERSECURITY STARTER PACK

This offer includes:

- ✔ Dark web scan with report
- ✔ Simulated phishing email
- ✔ Cybersecurity training for your staff
- ✔ Network walk-through
- ✔ One-page technology roadmap

Call 251-410-7601, email security@askbis.com or visit www.askbis.com/cybersecurity-starter-pack to redeem this offer!