The Unshakeable-Business Checklist from Movaci

Strategically Developed.
Security Expert-Approved.
Downtime Minimizing.

Keep your business running, no matter what the world throws at it.

Your business is more than products or service, it enables your team members to live the life they want, by answering the needs of your target market. But business-crippling disaster can strike in any form, at any time.

> *93 % of companies that lose data access for 10 days or more due to a disaster file for bankruptcy within a year, according to the National Archives & Records Administration in Washington.*

Your business faces multiple threats to its ongoing productivity and profitability, from server crashes to cyber-attacks, outages, or internet downtime to staff changeover. Therefore, you need an actionable plan that can be instantly implemented to ensure nothing shakes your business operations and profitability.

Enter our **Unshakeable Business Checklist**, a document strategically developed by our IT Security experts which minimizes or negates downtime for our clients, and now shared with you to keep your business running, no matter what the world throws at it.

We recommend completing this checklist immediately, and scheduling in regular annual or bi-annual reviews, depending on your business needs, goals or growth stage.

Need help completing this checklist? We're happy to lend a hand.
Schedule a FREE 30-MINUTE CONSULT with one of Movaci's Solutions Consultants today, available in English and Thai. Fill out the checklist below to ensure your business is unshakeable.

Your Movaci Team

RISK = CONSEQUENCE + LIKELIHOOD.
Consider some worst-case scenarios that could hit your business – Physical, Digital and Relational – and plan out how you would successfully respond to those situations to achieve the best possible results.

Section **1**
COUNT THE COST

Physical Assets

Account for both hardware and software - how are you actively protecting them? Create complete lists of all company hardware and devices, including identifier numbers, primary user and person responsible for maintaining it. This list should include (and add more if necessary).

- [ ] Computers (indicate desktop or laptop)
- [ ] Mobile Devices (indicate company or personal)
- [ ] Servers
- [ ] Routers, Modems, Phone Systems
- [ ] External Hard Drives
- [ ] Other

Pro-Tip: A list can be created as a password protected spreadsheet which is encrypted and accessible only to essential personnel. We also recommend noting the date of any change or revision on the sheet itself.

Digital Assets

Ensure a complete list of programs and business approved apps is maintained, including license keys for quick access. A complete list of approved programs and apps enables your IT Department or Partner to ensure protection from ever-increasing cyber attacks, and increases efficiency when onboarding new personnel or devices.

"To me, personal and corporate data are equally important. All sensitive data is worth protecting to ensure it doesn't fall into the wrong people's hands."
- Ray Panti, Movaci Security Services Manager

- [ ] Program or App Name
- [ ] License Key
- [ ] Developer
- [ ] Compatible Platforms
- [ ] List of devices the program is used on

Pro-Tip: Many Password Managers such as 1Password or LastPass include password-protected storage and management of software licenses, as well as login details.

Relational – Your People

Your people are the life and soul of your company. However, the "Human Firewall" tends to be the weakest link.

A comprehensive list of your employees, including job description, responsibility, access levels and device(s) used helps to ensure security, accountability and coverage for everyone involved. For simplicity, this list can link to the existing job descriptions and documents you already have in place.

- [ ] Staff Name
- [ ] Role + Position Description
- [ ] Access Level
- [ ] On-Call
- [ ] Device List

*Pro-Tip: A list can be created as a password protected spreadsheet which is encrypted and accessible only to essential personnel. We also recommend noting the date of any change or revision on the sheet itself.

Define "Emergency" and your Emergency Contacts

Emergency Response Action Plans are crucial to ensure business continuity. What strategies do you have in place to prevent emergency scenarios from shaking your business? Who is "on-call" if you become overwhelmed and need outside help/expertise, especially if you face a worst-case scenario that you haven't considered?

Each Emergency Response Action Plan you devise should include:

- [ ] Emergency Contact (responsible party that can implement a fix)
- [ ] Key Internal Stakeholder(s) who's ability to function will be impeded by situation, do Legal, Communications/PR Lead need to be involved etc?
- [ ] Approved External parties.

*Pro-Tip: Movaci's Global Service Desk is available 24/7 for our customers.

Maintain Your Unshakeable-Business List

This is not a checklist of things to do once and never worry about again. This is a checklist of all the factors to take into account repeatedly in order to refresh your recovery plan on a regular basis.

- [ ] A team member is onboarded or moves on
- [ ] A piece of hardware is swapped out, upgraded or retired
- [ ] A device is swapped out, upgraded or retired

*Pro-Tip: Here are a few of the recommendations we implement in our own policies:
Our _____ Unshakable Business Checklist will be reviewed and updated every _____ Months.
Relevant Documents will be updated whenever: _____

Ensuring an Unshakeable Business means your digital assets and information are not only up-to-date and encrypted, but securely backed up physically and in the cloud.

"You have to consider the worst-case scenario, where all the data is lost. How many hours of data changes are you willing to risk losing forever? That's what determines how often backups should take place."

- Paul Yawangsan, Movaci System Management Manager

Section **2**

STRATEGY

Establish your backup process and schedule

The person responsible for our backup and recovery process is:

[   ]

The person with secondary responsibility for our backup and recovery process is:

[   ]

Our Preferred Provider for unshakeable Business Continuity is Movaci ☐ Yes ☐ No

Our backups are (tick all that apply)   ☐ Encrypted backups   ☐ Physical – Onsite

☐ Physical – Offsite   ☐ Cloud-based

How reliable and durable is each form of backup?

[   ]

Server Backups are scheduled
(tick and detail all that apply)

☐ Hourly

☐ Multiple-times daily
(list how many daily backups)   [   ]

☐ Once Daily   ☐ Weekly

Staff Computer Backups are scheduled

☐ Hourly

☐ Multiple-times daily
(list how many daily backups)   [   ]

☐ Once Daily   ☐ Weekly

Staff Device Backups are scheduled

☐ Hourly

☐ Multiple-times daily
(list how many daily backups)   [   ]

☐ Once Daily   ☐ Weekly

This year, **40% of small to medium sized businesses** that manage their own network and use the Internet for more than e-mail **will have their network accessed by a hacker**, and **more than 50% won't even know they were attacked**.
(Source: Gartner Group)

Test Your firewalls
Challenge and push your IT system firewalls in order to prove their reliability for when a real threat occurs.

Section 3
IMPLEMANTATION

Digital Firewalls

Latest Firewall Test occurred on (date): _____

Next Firewall Test is scheduled on (date): _____

Human Firewalls

Your team members are the most important part of your business, but they are also your greatest IT liability. It is therefore imperative for them to be security conscious, and security competent.
Assess your employees' habits and security-awareness in order to determine how they would perform in a security-risk scenario, especially when faced with phishing and ransomware attacks. Pay special attention to safeguarding all Cloud-based services

Our Staff have received
IT Security Awareness Training

☐ Yes (date) _____

☐ No   Schedule your IT SecurityAwareness Training with Movaci

Zero Trust Security Measures

Evaluate the level of zero trust security which you have integrated into your security system to test every access attempt of sensitive data.

Multi-factor authentication is required and enabled on all

Company Desktop Computers   ☐ Yes   ☐ No

Company or Company-used Laptops   ☐ Yes   ☐ No

Company or Personal Devices used for Company Purposes   ☐ Yes   ☐ No

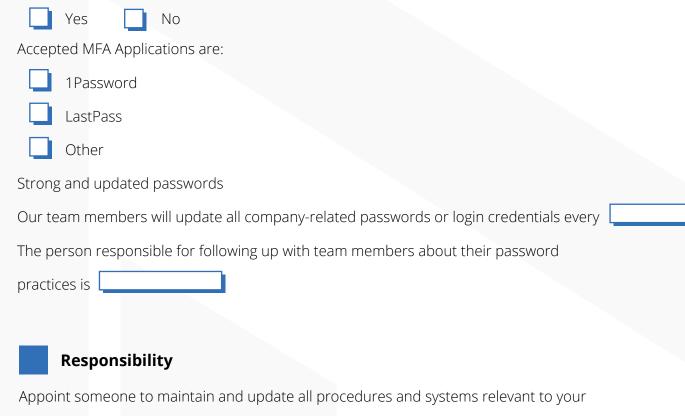Accepted MFA Applications are: ☐ Microsoft Authenticator

                                        ☐ Google Authenticator

                                        ☐ Other

Password Managers are Required, Installed and Updated on Company Hardware

☐ Yes   ☐ No

Accepted MFA Applications are:

☐ 1Password

☐ LastPass

☐ Other

Strong and updated passwords

Our team members will update all company-related passwords or login credentials every [   ]

The person responsible for following up with team members about their password

practices is [   ]

■ Responsibility

Appoint someone to maintain and update all procedures and systems relevant to your

Unshakeable-Business Checklist on a daily basis. Key responsibilities include:

☐ Scheduled testing of all security measures to determine weak points in the structure

☐ Keeping your systems and employees in compliance with constantly-changing internet and business regulations
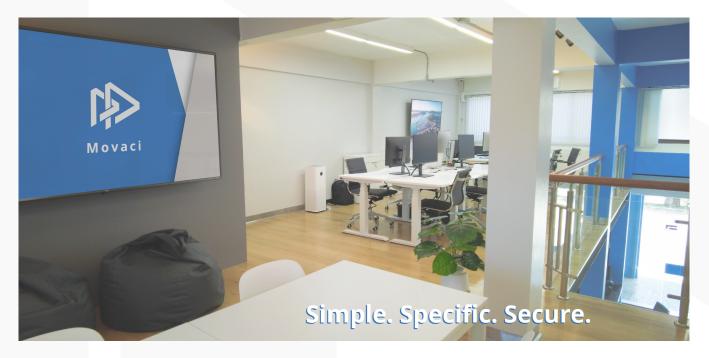
☐ Staying current on hacker tactics and new information concerning online business strategies

When you implement, and regularly review and update the points on this Unshakeable-Business Checklist, your businesses is hardened against all forms of threats to your productivity and profitability.

We hope this checklist helps you as much as it has helped our clients remain unshakeable.

Simple. Specific. Secure.

Every entity with a digital footprint, from Enterprise to local Non-profit, requires an IT Solution which their team can simply use, meets and scales with their business or organizational needs, and ensures all of their assets are protected from both internal and external threats.

But for many organizations, simply adapting to the ever-changing digital landscape is a necessary distraction, which keeps them from focusing on their core mission, and hamstrings productivity, profit and growth.

Therefore, they need a Solutions Provider that will custom-fit the right solution to help them achieve their goals efficiently and securely in the present, and which scales with them for the future.

Movaci is the Preferred Partner in IT Solutions for companies in over 30 countries and across every major industry and sector. Developed and managed from end-to-end by highly certified and uniquely experienced staff, we craft **tailored IT Solutions to provide you with the highest level of functionality, reliability, and security to ensure your optimal outcome.**

Our unique approach and global experience matched with industry-leading technology are perfectly aligned to meet the ever-changing IT needs of your business.

Find out why companies like yours in more than 30 countries have made us their Preferred Partner in IT Security at movaci.com/clients/