

## Comprsa

# Small Business Cybersecurity Risk Assessment

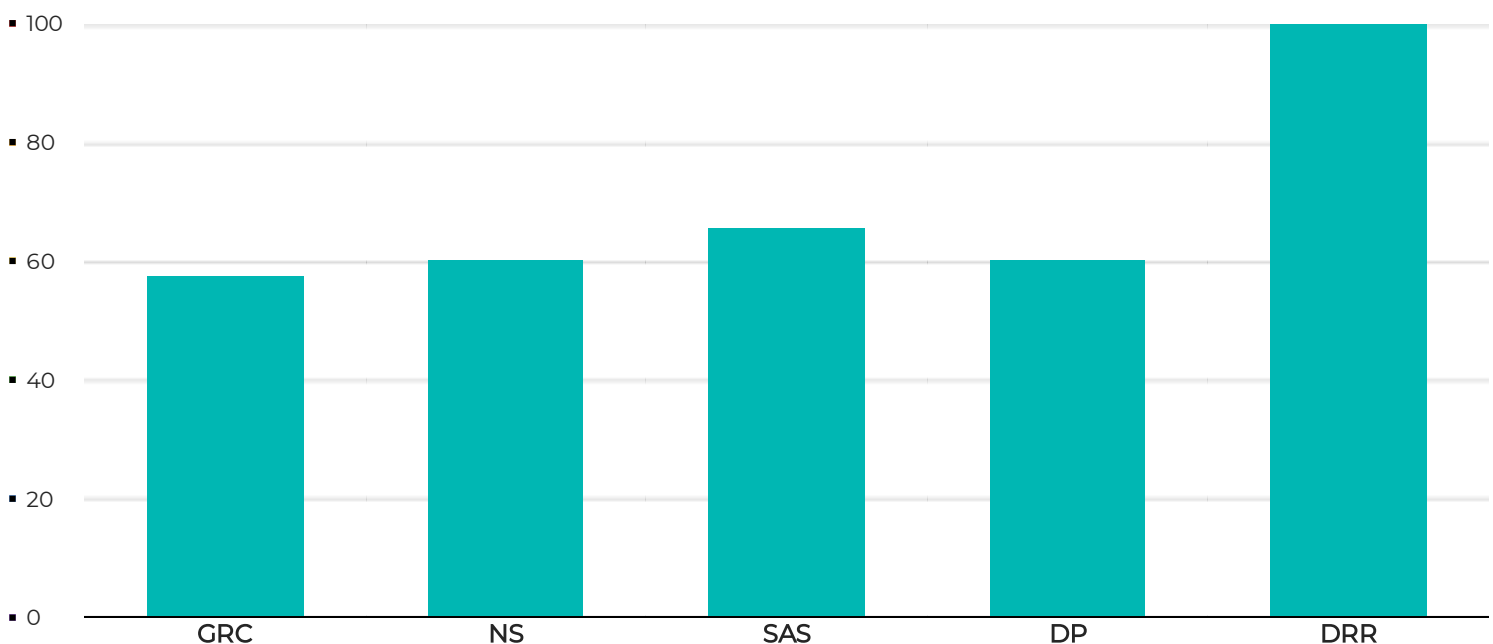
Thank you for taking our Small Business Cybersecurity Survey! Using your responses, we have determined your risk level in five key cybersecurity areas by assigning a value of High to Low to each response where “strongly disagree” = High and “strongly agree” = Low. Each category was then averaged to determine your overall risk level. We provide insights and best practices customized for you so you can increase the security posture of your business starting today!



### Overall cybersecurity risk level

Based upon your responses we determined your overall cybersecurity risk level is medium. A summary of your risk in each cybersecurity category is shown below. Detailed responses and feedback follow on the next pages.

Overall cybersecurity risk level = Medium



## Governance, Risk, and Compliance

### Risk Level M

Statement	Response	Score
Our company has a documented Remote Access policy	Sometimes	M
Our company has a documented Change Management policy	Sometimes	M
We understand our compliance obligations and regularly assess our adherence to those requirements	Neutral	M
We have purchased cyber liability insurance	Neutral	M
Our company has a documented Acceptable Use of IT Assets policy	Sometimes	M
We provide security training to our employees	Only at onboarding	L
Our company has a documented IT Asset Management policy	Sometimes	M
Our company has a documented Data Classification and Handling policy	Sometimes	M
Our company has a documented Third-Party Management policy	Sometimes	M
Our company has a documented Identity and Access Management policy	Sometimes	M
Our company has a documented Security Awareness and Training policy	Sometimes	M
Our company has a documented Backup and Recovery policy	Sometimes	M
We assess our third-party service providers and suppliers to evaluate their security controls and potential risk	Neutral	M
The last time we performed an IT security assessment was	3+ years ago	L
Our company has a documented Data Retention and Disposal policy	Sometimes	M



Your self-assessment indicates your current governance, risk, and compliance capabilities are mature. Cybersecurity is not just an IT risk, and governance, risk, and compliance processes are important in appropriately managing cybersecurity risk across the entire organization.

#### Best Practices:

- 1.
2. Best practices:
3. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.
4. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.
5. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.

## Network Security

### Risk Level M

Statement	Response	Score
The last time we performed an external penetration test on our internet facing systems was	3+ years ago	M
We have implemented remote access solutions for our internal systems	Sometimes	M
Our company has a well documented inventory of our network infrastructure	Neutral	M
We have implemented firewalls with Intrusion Detection and Intrusion Prevention capabilities enabled	Neutral	M
We require multi-factor authentication for our remote access solutions	Neutral	M



Your self-assessment indicates your current network security capabilities are mature. Cybersecurity risks must be managed in a layered manner, with network security being the foundation on which the rest of your technical security controls rely. .

Best Practices:

## System and Application Security

### Risk Level M

Statement	Response	Score
Our company has a well documented inventory of our systems and applications	Neutral	M
Access to our internal applications is controlled through Active Directory, not locally managed user accounts	Sometimes	H
We utilize Active Directory or another centralized authentication source for managing employee access	Sometimes	M
We develop proprietary applications for internal use	Sometimes	M
We have a documented change management process	Sometimes	M
The last time we performed internal vulnerability scanning on our internal systems and applications was	3+ years ago	M
We have implemented antivirus/antimalware solutions on end user computers	Sometimes	M



Your self-assessment indicates your current network security capabilities are mature. Cybersecurity risks must be managed in a layered manner, with network security being the foundation on which the rest of your technical security controls rely. .

Best Practices:

## Data Protection

### Risk Level M

Statement	Response	Score
We securely dispose of sensitive data when it is no longer needed	Neutral	M
We encrypt sensitive data when stored at rest, whether on end user workstations, removeable media, or internal databases.	Neutral	M
We require third-parties that we share sensitive data with to meet minimum data protection standards	Neutral	M
We encrypt sensitive data when transmitted internally or to third-parties	Neutral	M
We perform regular data backups	Sometimes	M
Our company maintains an inventory of where our most sensitive data is stored, processed, or transmitted.	Neutral	M



Your self-assessment indicates your current network security capabilities are mature. Cybersecurity risks must be managed in a layered manner, with network security being the foundation on which the rest of your technical security controls rely. .

Best Practices:

## Detection, Response, and Recovery

### Risk Level H

Statement	Response	Score
We last tested our business continuity, disaster recovery, and cybersecurity incident response plans	Within the last 12 months	H
Our IT team receives an alert when a security event occurs	Strongly Agree	H
Our company has documented business continuity and disaster recovery plans	Strongly Agree	H
Our company has documented cybersecurity incident response plans	Strongly Agree	H



Your self-assessment indicates your current governance, risk, and compliance capabilities are mature. Cybersecurity is not just an IT risk, and governance, risk, and compliance processes are important in appropriately managing cybersecurity risk across the entire organization.




Best Practices:

- 1.
2. Best practices:
3. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.
4. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.
5. Your company should implement an employee training program, with security training occurring during new hire onboarding and at least once per year thereafter.

## For More Information

Please contact at Email [Brian.Nichols@bakertilly.com](mailto:Brian.Nichols@bakertilly.com) For More Information

### CONNECT WITH US

-  @BakerTillyUS
-  Baker Tilly US, LLP
-  [bakertilly.com](https://www.bakertilly.com)

### ABOUT BAKER TILLY

Baker Tilly US, LLP (Baker Tilly) is a leading advisory, tax and assurance firm whose specialized professionals guide clients through an ever-changing business world, helping them win now and anticipate tomorrow. Headquartered in Chicago, Baker Tilly, and its affiliated entities, have operations in North America, South America, Europe, Asia and Australia.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought. Tax information, if any, contained in this communication was not intended or written to be used by any person for the purpose of avoiding penalties, nor should such information be construed as an opinion upon which any person may rely. The intended recipients of this communication and any attachments are not subject to any limitation on the disclosure of the tax treatment or tax structure of any transaction or matter that is the subject of this communication and any attachments. Baker Tilly US, LLP trading as Baker Tilly is a member of the global network of Baker Tilly International Ltd., the members of which are separate and independent legal entities. © 2022 Baker Tilly US, LLP