

# 10

## Cybersecurity Misconceptions for Small & Medium - Sized Organizations

### Misconception #1

My data [or the data I have access to] isn't valuable



All data is valuable

### Misconception #2

Cybersecurity is a technology issue



Cybersecurity is best approached with a mix of employee training; clear, accepted policies and procedures and implementation of current technologies

### Misconception #3

Cybersecurity requires a huge financial investment



Many efforts to protect your data require little or no financial investment

### Misconception #4

Outsourcing to a vendor washes your hands of liability during a cyber incident



You have a legal and ethical responsibility to protect sensitive data

### Misconception #5

Cyber breaches are covered by general liability insurance



Many standard insurance policies do **not** cover cyber incidents or data breaches

### Misconception #6

Cyberattacks always come from external factors



Succinctly put, cyberattacks do not always come from external factors

### Misconception #7

Younger people are better at cybersecurity than others



Age is not directly correlated to better cybersecurity practices

### Misconception #8

Compliance with industry standards is sufficient for a security strategy



Simply complying with industry standards does not equate to a robust cybersecurity strategy for an organization

### Misconception #9

Digital and physical security are separate things altogether



Do not discount the importance of physical security

### Misconception #10

New software and devices are secure when I buy them



Just because something is new, does not mean it is secure