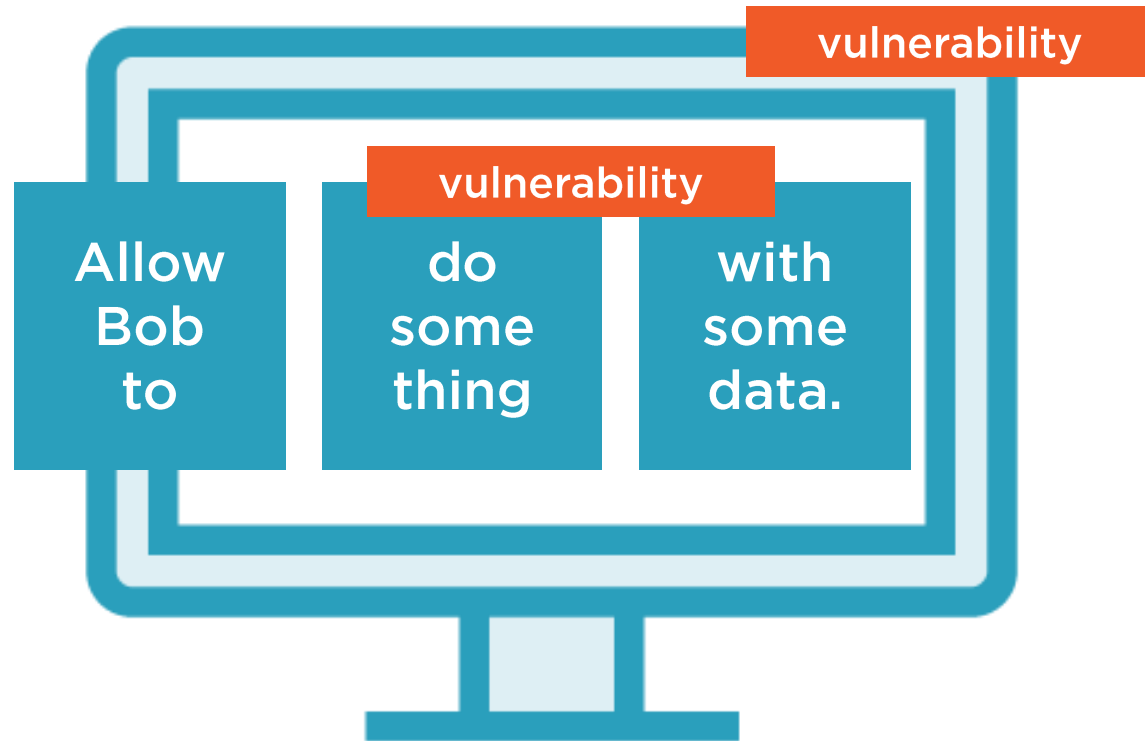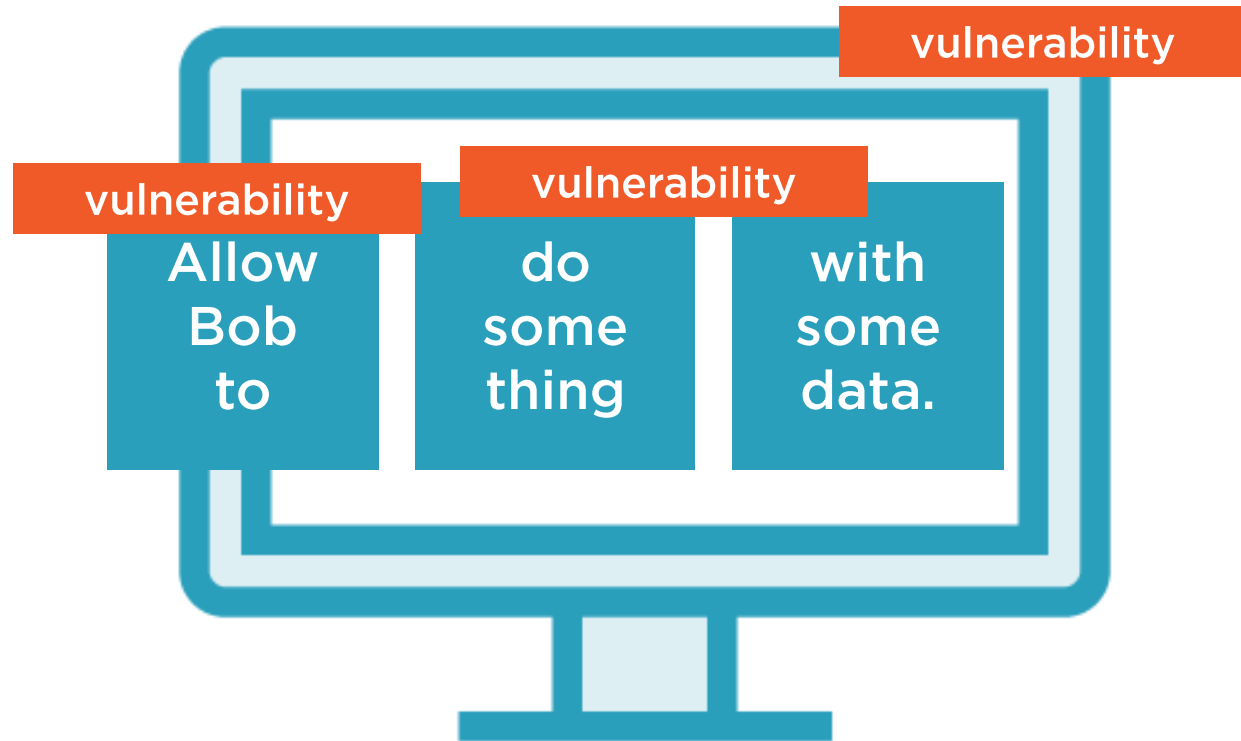Malware: Malicious software
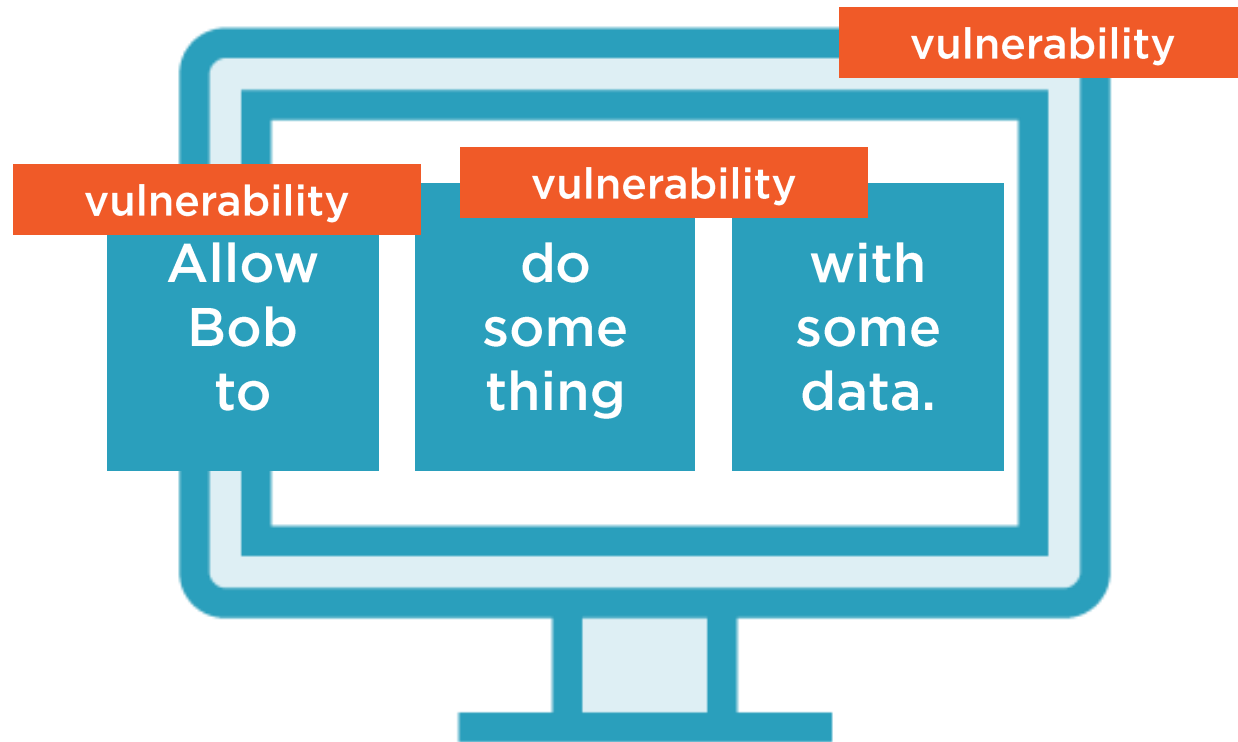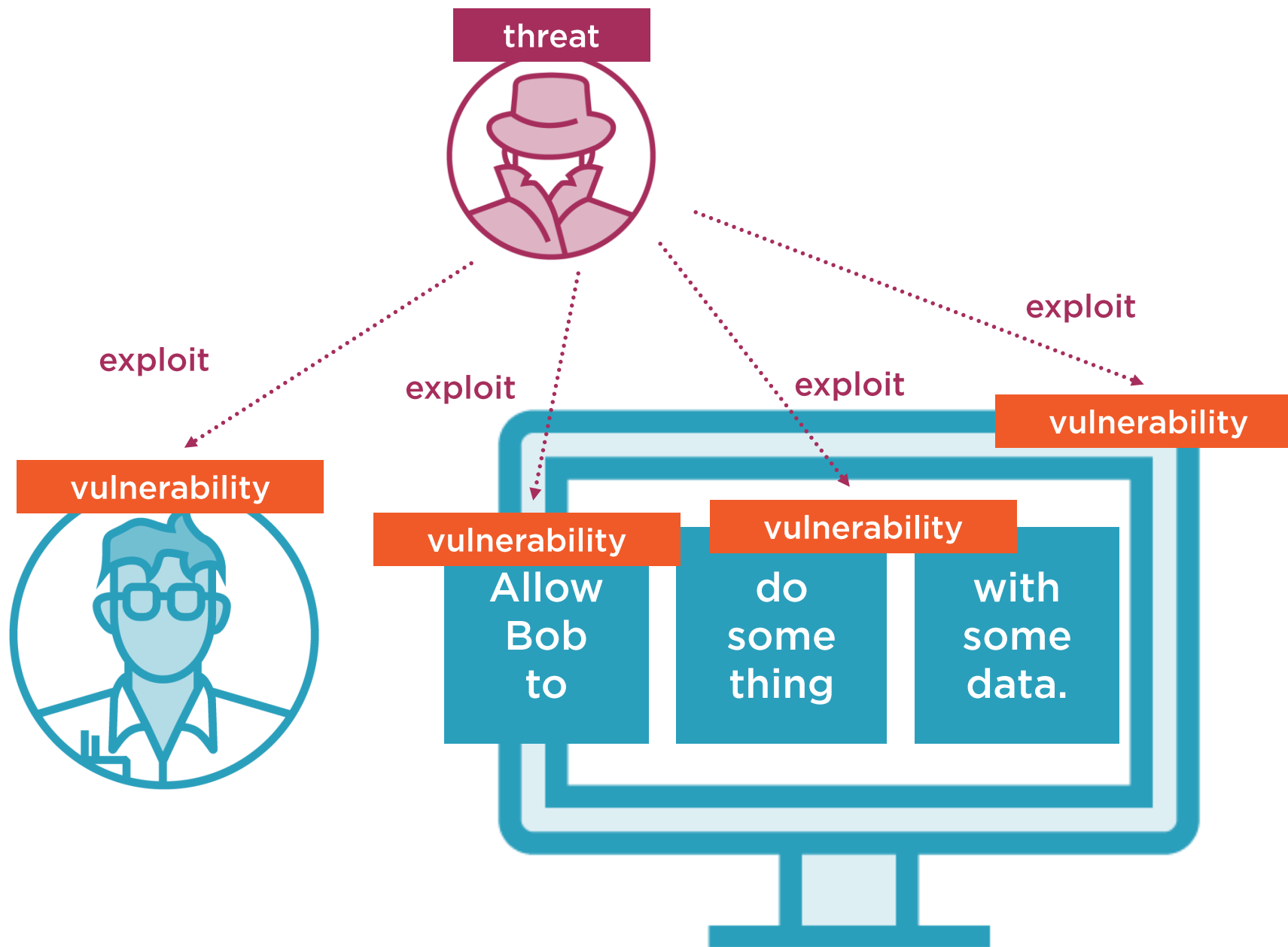
threat

vulnerability

vulnerability

vulnerability

vulnerability

Allow Bob to do some thing with some data.

# Control

Prevents a threat actor exploiting a vulnerability

# Cyber Risk Assessment for an Information Asset

Probability of Attack

High risk cyber event

Low risk cyber event

Impact to the Organization

| Financial ? | Reputation ? | Regulatory ? | Operational ? |

# Cyber Risk Assessment for an Information Asset

**Motivation of attacker ?**

**Probability of Attack**

**High risk cyber event** ●

**Low risk cyber event** ●

**Impact to the Organization**

**Financial ?**    **Reputation ?**    **Regulatory ?**    **Operational ?**

# Cyber Risk Assessment for an Information Asset

**Motivation of attacker ?**

Confidentiality ?

High risk cyber event

Probability of Attack

Low risk cyber event

Impact to the Organization

Financial ? | Reputation ? | Regulatory ? | Operational ?

Confidentiality ?

# Cyber Risk Assessment for an Information Asset

**Motivation of attacker ?**

Confidentiality ?

Integrity ?

Probability of Attack

High risk cyber event

Low risk cyber event

Impact to the Organization

Financial ?   Reputation ?   Regulatory ?   Operational ?

Confidentiality ?   Integrity ?

# Cyber Risk Assessment for an Information Asset

**Motivation of attacker ?**

Confidentiality ?

Integrity ?

Availability ?

Probability of Attack

High risk cyber event

Low risk cyber event

Impact to the Organization

**Financial ?**  **Reputation ?**  **Regulatory ?**  **Operational ?**

Confidentiality ?  Integrity ?  Availability ?

# Cyber Risk Assessment for an Information Asset

**Motivation of attacker ?**

Confidentiality ?

Integrity ?

Availability ?

**Vulnerabilities ?**

Probability of Attack

High risk cyber event

Low risk cyber event

Impact to the Organization

**Financial ?** **Reputation ?** **Regulatory ?** **Operational ?**

Confidentiality ? Integrity ? Availability ?

# Cyber Risk Assessment for an Information Asset



Motivation of attacker ?

Confidentiality ?

Integrity ?

Availability ?

Vulnerabilities ?

Controls ?

Probability of Attack

High risk cyber event

Low risk cyber event

Impact to the Organization

Financial ?    Reputation ?    Regulatory ?    Operational ?

Confidentiality ?    Integrity ?    Availability ?

Controls can be preventative, detective or corrective

**Preventative controls stop bad things happening**
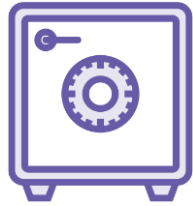
Detective controls detect bad things happening

Corrective controls are used after bad things have happened

US National Institute of Standards and Technology (NIST)

# NIST Cyber Security Framework

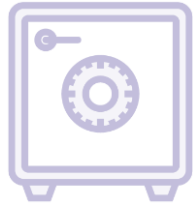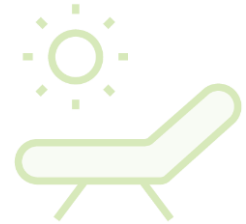| Identify | Protect | Detect | Respond | Recover |
|----------|---------|--------|---------|---------|
| Know how you can be attacked | Put controls in place to prevent the attack | Put controls in place to identify when you've been attacked | Know how you can stop the attack once you've detected it | Plan how you will restore normal operations |

# NIST Cyber Security Framework

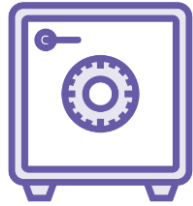| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Know how you can be attacked | Put controls in place to prevent the attack | Put controls in place to identify when you've been attacked | Know how you can stop the attack once you've detected it | Plan how you will restore normal operations |

# NIST Cyber Security Framework

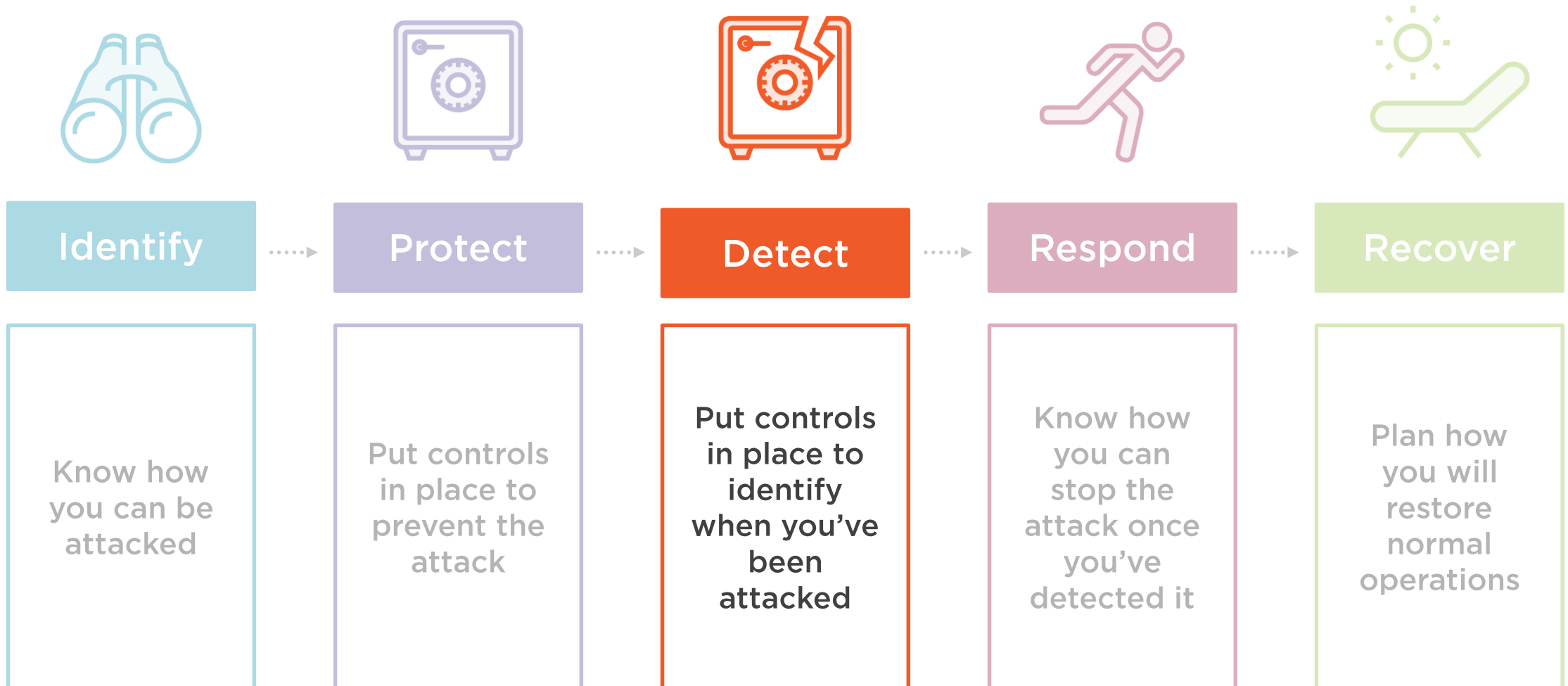| Identify | Protect | Detect | Respond | Recover |
|---|---|---|---|---|
| Know how you can be attacked | Put controls in place to prevent the attack | Put controls in place to identify when you've been attacked | Know how you can stop the attack once you've detected it | Plan how you will restore normal operations |

# NIST Cyber Security Framework

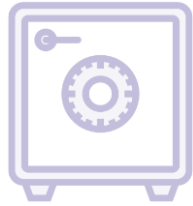| Identify | Protect | Detect | Respond | Recover |
|----------|---------|--------|---------|---------|
| Know how you can be attacked | Put controls in place to prevent the attack | **Put controls in place to identify when you've been attacked** | Know how you can stop the attack once you've detected it | Plan how you will restore normal operations |

# NIST Cyber Security Framework

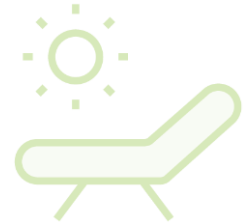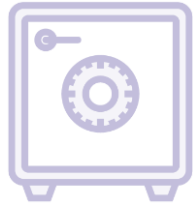| Identify | Protect | Detect | Respond | Recover |
|----------|---------|--------|---------|---------|
| Know how you can be attacked | Put controls in place to prevent the attack | Put controls in place to identify when you've been attacked | **Know how you can stop the attack once you've detected it** | Plan how you will restore normal operations |

# NIST Cyber Security Framework

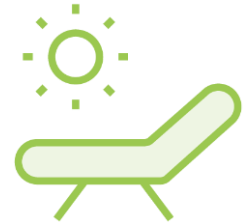| Identify | Protect | Detect | Respond | Recover |
|----------|---------|--------|---------|---------|
| Know how you can be attacked | Put controls in place to prevent the attack | Put controls in place to identify when you've been attacked | Know how you can stop the attack once you've detected it | **Plan how you will restore normal operations** |

# Control Frameworks

Helpful collections
of pre-selected controls

# Control Frameworks

Mandatory collections
of pre-selected controls
(e.g. regulatory)

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

Payment Card Industry
Data Security Standard (PCI DSS)

Health Insurance Portability and
Accountability Act (HIPAA)

CIS 20 Critical Controls

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## International Standards Organization
## ISO 27001 / 27002

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## Federal Financial Institutions Examination Council
## Cyber Security Assessment

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## Payment Card Industry
## Data Security Standard (PCI DSS)

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## Health Insurance Portability and Accountability Act
## HIPAA

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## Center for Internet Security
## 20 Critical Controls for Cyber Security

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

## UK National Cyber Security Centre
## Cyber Essentials

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

**Australian Cyber Security Centre "Essential Eight"**

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"

# Common Control Frameworks

ISO 27001 / 27002

FFIEC Cyber Security Assessment

Payment Card Industry
Data Security Standard (PCI DSS)

Health Insurance Portability and
Accountability Act (HIPAA)

CIS 20 Critical Controls

UK NCSC Cyber Essentials

Australian CSC "Essential Eight"