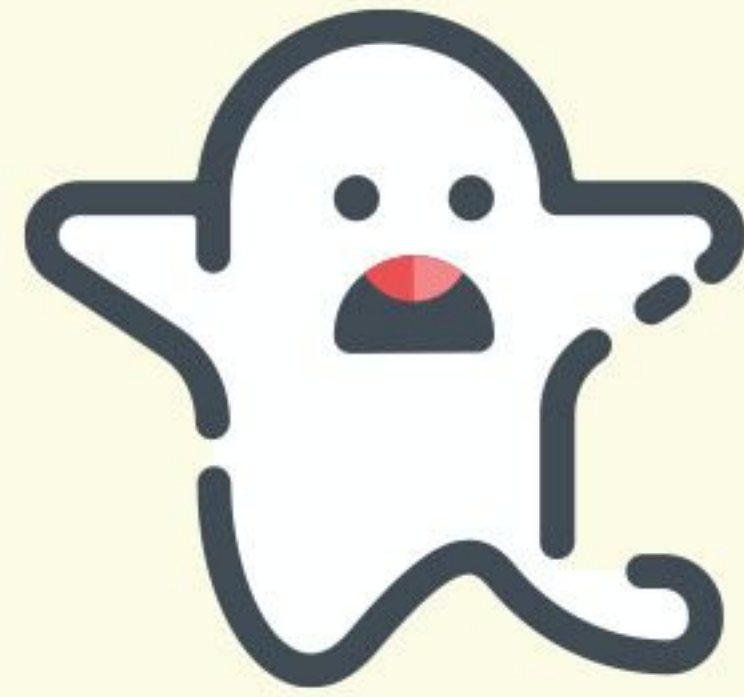
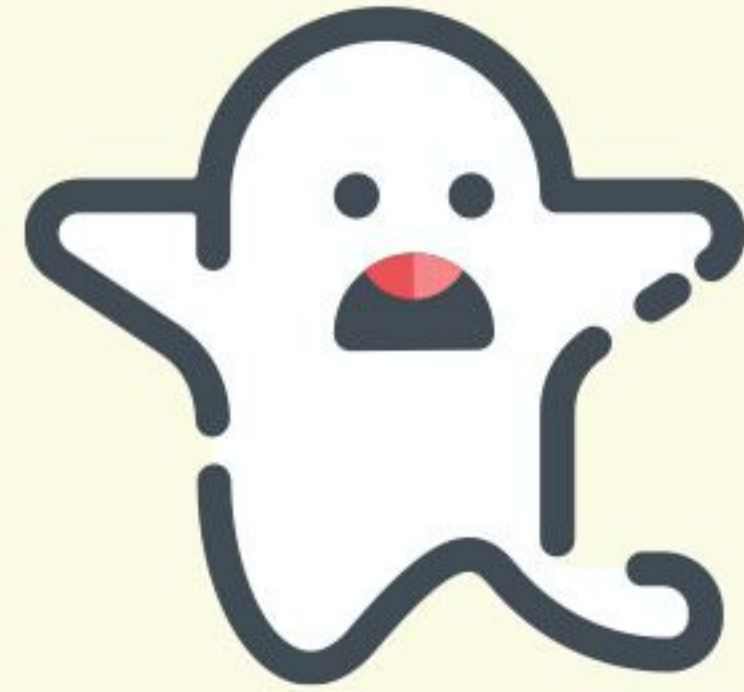


# Risk Decisions in an Imperfect World





**Will this decision haunt me?**



**Will this decision haunt me?  
Did I even make a decision?**



**Something happened**  
**(or you're about to make it happen)**



**Impact of the event**



**Likelihood it occurs**



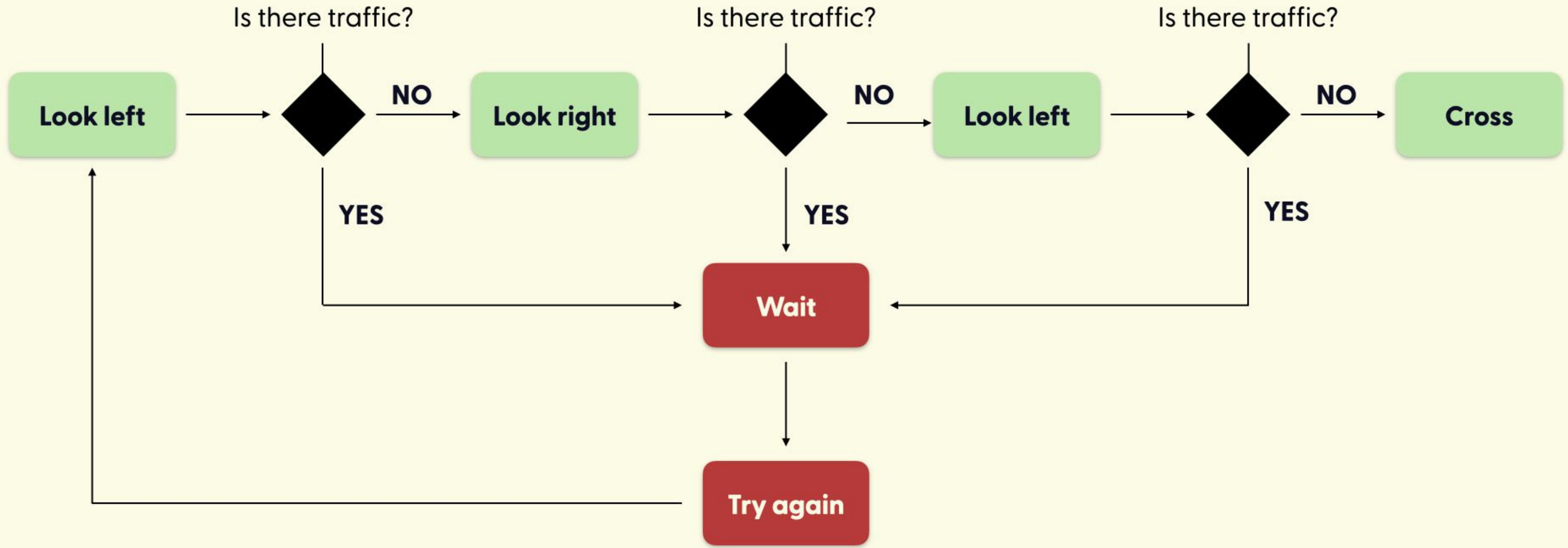
**Are you ok with that?**



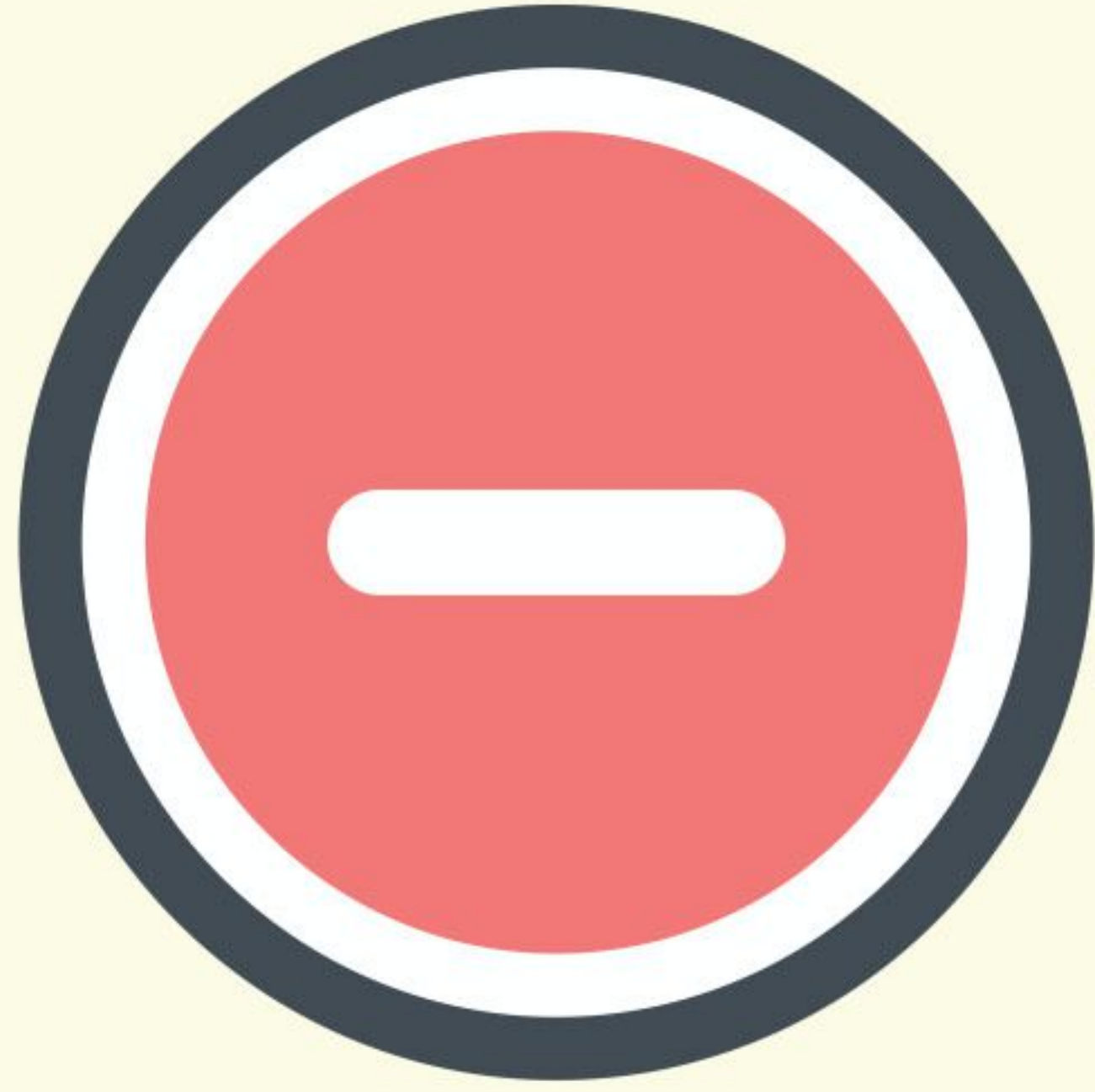


# Crossing the street

\* For countries that drive on the right hand side








**Is this too risky?**



**We need data**



**9,000**

**Dead 1989–2009**

**64%**

**Were trying to  
cross the road**



**~300 fatalities/year**





**2017**





**~300 fatalities/year**



**Is our data complete?**  
**(-ish, at least reasonable comprehensive)**

2007



2017

**~300**

Pedestrian fatalities

**284**

**27.5**

Registered cars  
(in millions)

**34.3**

**412.5**

Kilometers driven  
(in billions)

**516**

**24.32% decrease**

# Decision Workflow



**Impact of the event**



**Likelihood it occurs**



**Is that too risky?**



**Apply mitigations**

# Decision Workflow



**Impact of the event**



*Gather data & review*



**Likelihood it occurs**



*Gather data & review*



**Is that too risky?**



*Gather data & review*



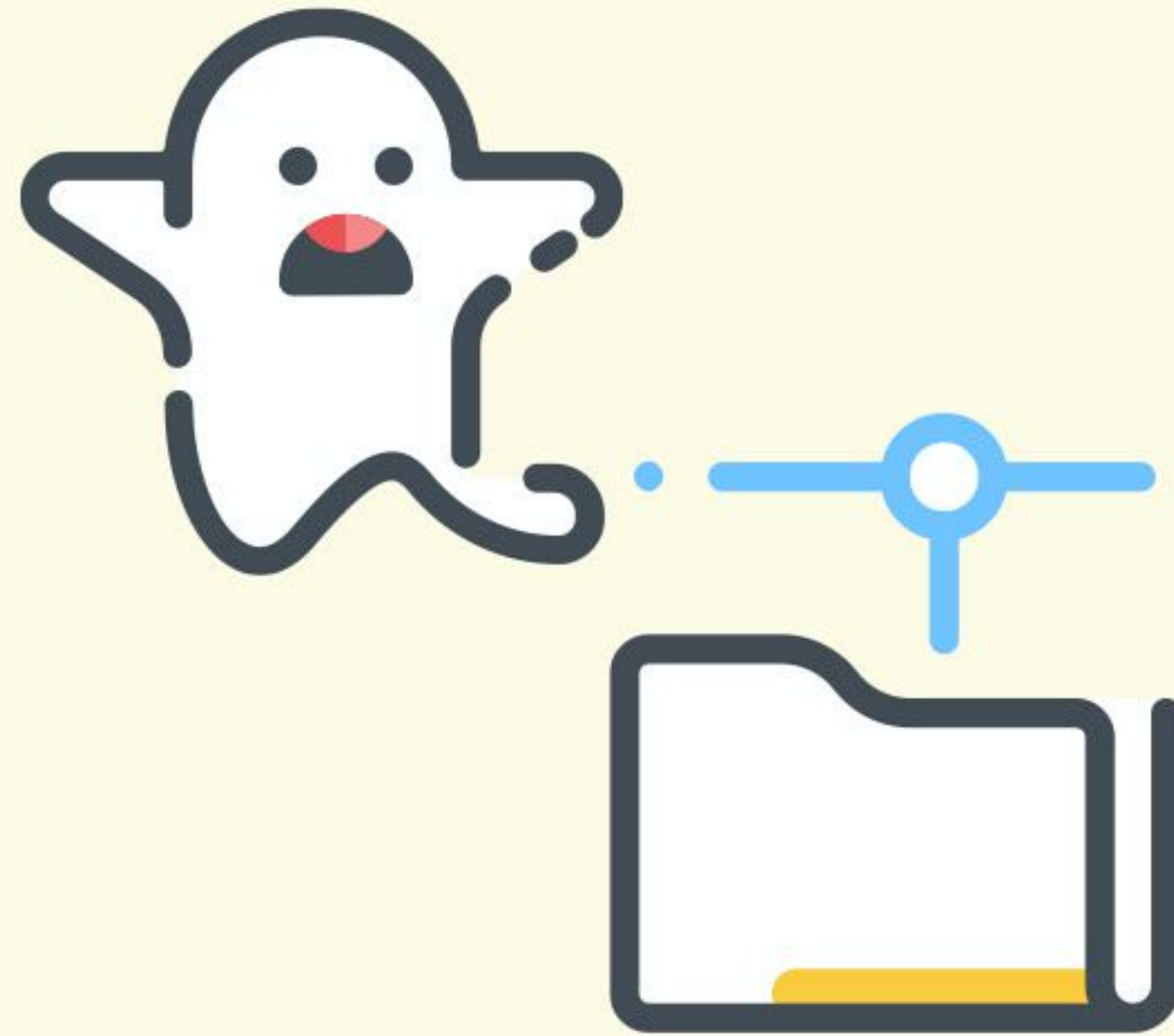
**Apply mitigations**





# **CVE-2020-0796**

**(CVSS score 9/10)**



# SMBGhost

(CVSS score 9/10)



# Exploiting CVE-2020-0796

*(Echoes of WannaCry)*

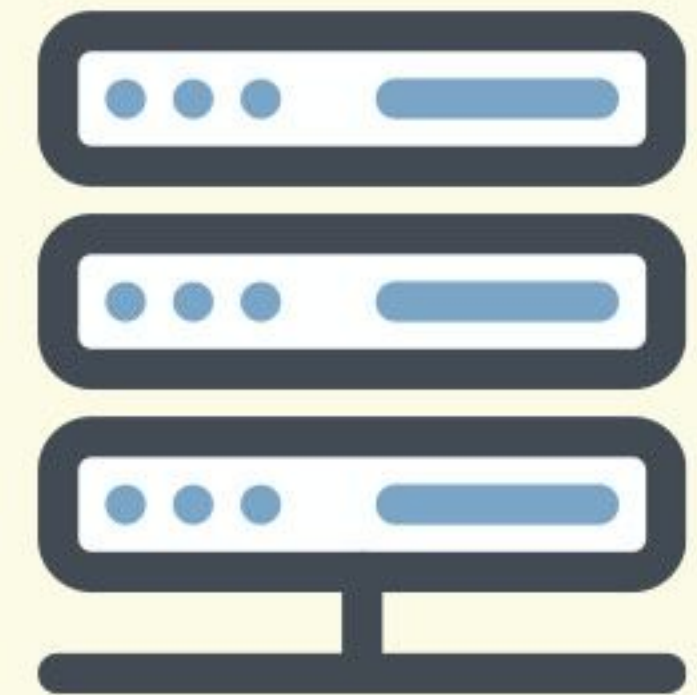
Attacker owns system



Cybercriminal



Crafted packet



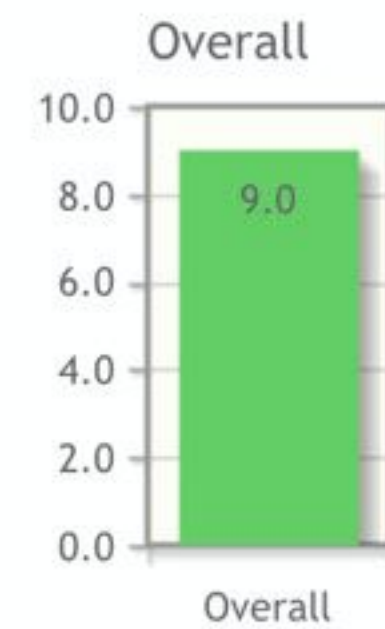
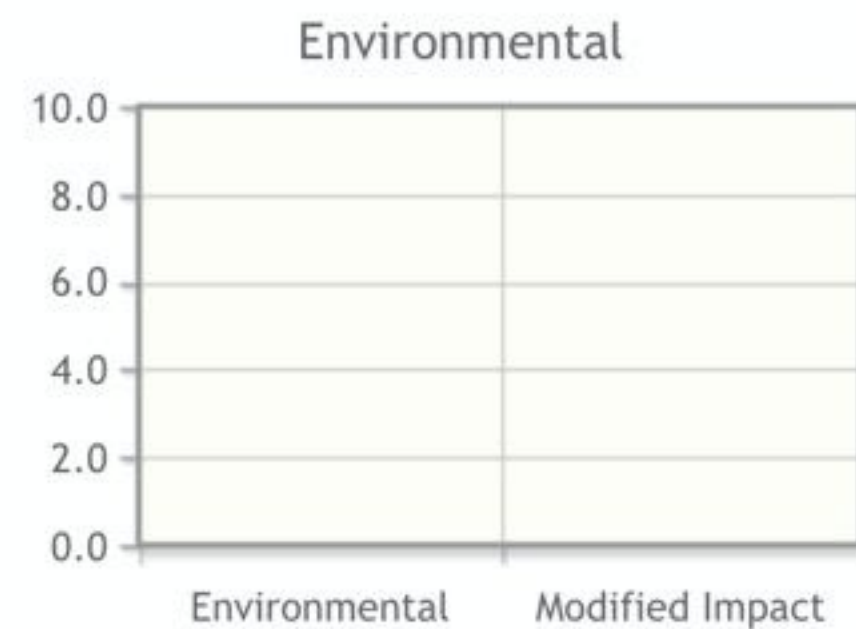
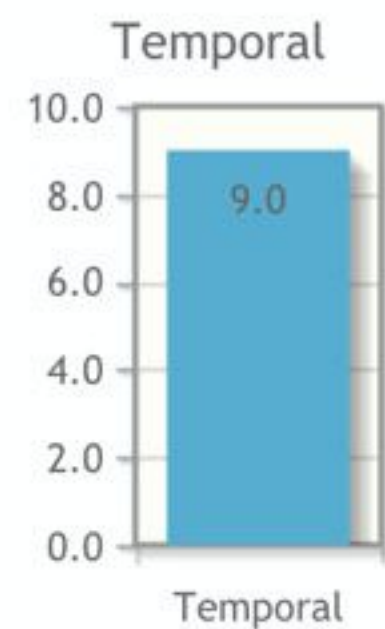
Windows File Server

VULNERABILITY METRICS

CVSS Version 3.0 CVSS Version 3.1

### Common Vulnerability Scoring System Calculator

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



**CVSS Base Score: 10.0**  
 Impact Subscore: 6.0  
 Exploitability Subscore: 3.9  
**CVSS Temporal Score: 9.0**  
 CVSS Environmental Score: NA  
 Modified Impact Subscore: NA  
**Overall CVSS Score: 9.0**

Show Equations

CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

## Base Score Metrics

### Exploitability Metrics

#### Attack Vector (AV)\*

Network (AV:N) Adjacent Network (AV:A) Local (AV:L) Physical (AV:P)

#### Attack Complexity (AC)\*

Low (AC:L) High (AC:H)

#### Privileges Required (PR)\*

None (PR:N) Low (PR:L) High (PR:H)

#### User Interaction (UI)\*

None (UI:N) Required (UI:R)

#### Scope (S)\*

Unchanged (S:U) Changed (S:C)

### Impact Metrics

#### Confidentiality Impact (C)\*

None (C:N) Low (C:L) High (C:H)

#### Integrity Impact (I)\*

None (I:N) Low (I:L) High (I:H)

#### Availability Impact (A)\*

None (A:N) Low (A:L) High (A:H)

\* - All base metrics are required to generate a base score.

## Temporal Score Metrics

### Exploitability (E)

Not Defined (E:X) Unproven that exploit exists (E:U) Proof of concept code (E:P) Functional exploit exists (E:F) High (E:H)

### Remediation Level (RL)

Not Defined (RL:X) Official fix (RL:O) Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

### Report Confidence (RC)

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) Confirmed (RC:C)

## Environmental Score Metrics

### Base Modifiers

#### Attack Vector (AV)

Not Defined (MAV:X) Network (MAV:N) Adjacent Network (MAV:A)

### Impact Metrics

#### Confidentiality Impact (C)

Not Defined (MC:X) None (MC:N) Low (MC:L)

### Impact Subscore Modifiers

#### Confidentiality Requirement (CR)

Not Defined (CR:X) Low (CR:L)

Low (AC:L) High (AC:H)

**Privileges Required (PR)\***

None (PR:N) Low (PR:L) High (PR:H)

**User Interaction (UI)\***

None (UI:N) Required (UI:R)

None (C:N) Low (C:L) High (C:H)

**Integrity Impact (I)\***

None (I:N) Low (I:L) High (I:H)

**Availability Impact (A)\***

None (A:N) Low (A:L) High (A:H)

\* - All base metrics are required to generate a base score.

## Temporal Score Metrics

**Exploitability (E)**

Not Defined (E:X) Unproven that exploit exists (E:U) **Proof of concept code (E:P)** Functional exploit exists (E:F) High (E:H)

**Remediation Level (RL)**

Not Defined (RL:X) **Official fix (RL:O)** Temporary fix (RL:T) Workaround (RL:W) Unavailable (RL:U)

**Report Confidence (RC)**

Not Defined (RC:X) Unknown (RC:U) Reasonable (RC:R) **Confirmed (RC:C)**

## Environmental Score Metrics

### Base Modifiers

**Attack Vector (AV)**

**Not Defined (MAV:X)** Network (MAV:N) Adjacent Network (MAV:A)  
Local (MAV:L) Physical (MAV:P)

**Attack Complexity (AC)**

**Not Defined (MAC:X)** Low (MAC:L) High (MAC:H)

**Privileges Required (PR)**

**Not Defined (MPR:X)** None (MPR:N) Low (MPR:L) High (MPR:H)

**User Interaction (UI)**

**Not Defined (MUI:X)** None (MUI:N) Required (MUI:R)

**Scope (S)**

**Not Defined (MS:X)** Unchanged (MS:U) Changed (MS:C)

### Impact Metrics

**Confidentiality Impact (C)**

**Not Defined (MC:X)** None (MC:N) Low (MC:L)  
High (MC:H)

**Integrity Impact (I)**

**Not Defined (MI:X)** None (MI:N) Low (MI:L)  
High (MI:H)

**Availability Impact (A)**

**Not Defined (MA:X)** None (MA:N) Low (MA:L)  
High (MA:H)

### Impact Subscore Modifiers

**Confidentiality Requirement (CR)**

**Not Defined (CR:X)** Low (CR:L)  
Medium (CR:M) High (CR:H)

**Integrity Requirement (IR)**

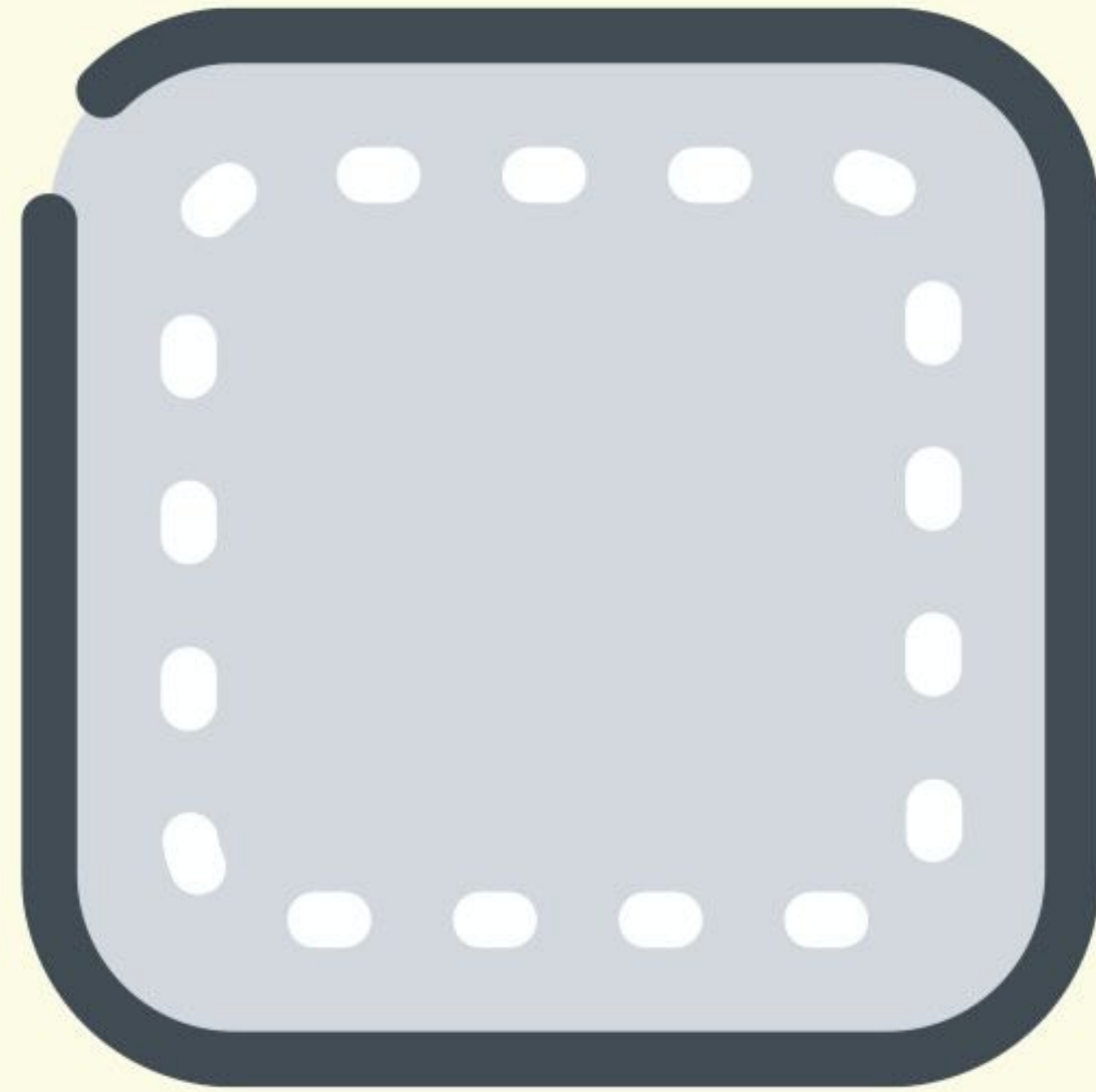
**Not Defined (IR:X)** Low (IR:L) Medium (IR:M)  
High (IR:H)

**Availability Requirement (AR)**

**Not Defined (AR:X)** Low (AR:L)  
Medium (AR:M) High (AR:H)



**Is this too risky?**



**43.8%**

**(Completed patches in 90d)**

# Decision Workflow



**Impact of the event**

—————> Attacker gains control of system

↓  
*Gather data & review*

—————> CVSS & vendor recommendations



↓  
**Likelihood it occurs**

—————> **???**

↓  
*Gather data & review*

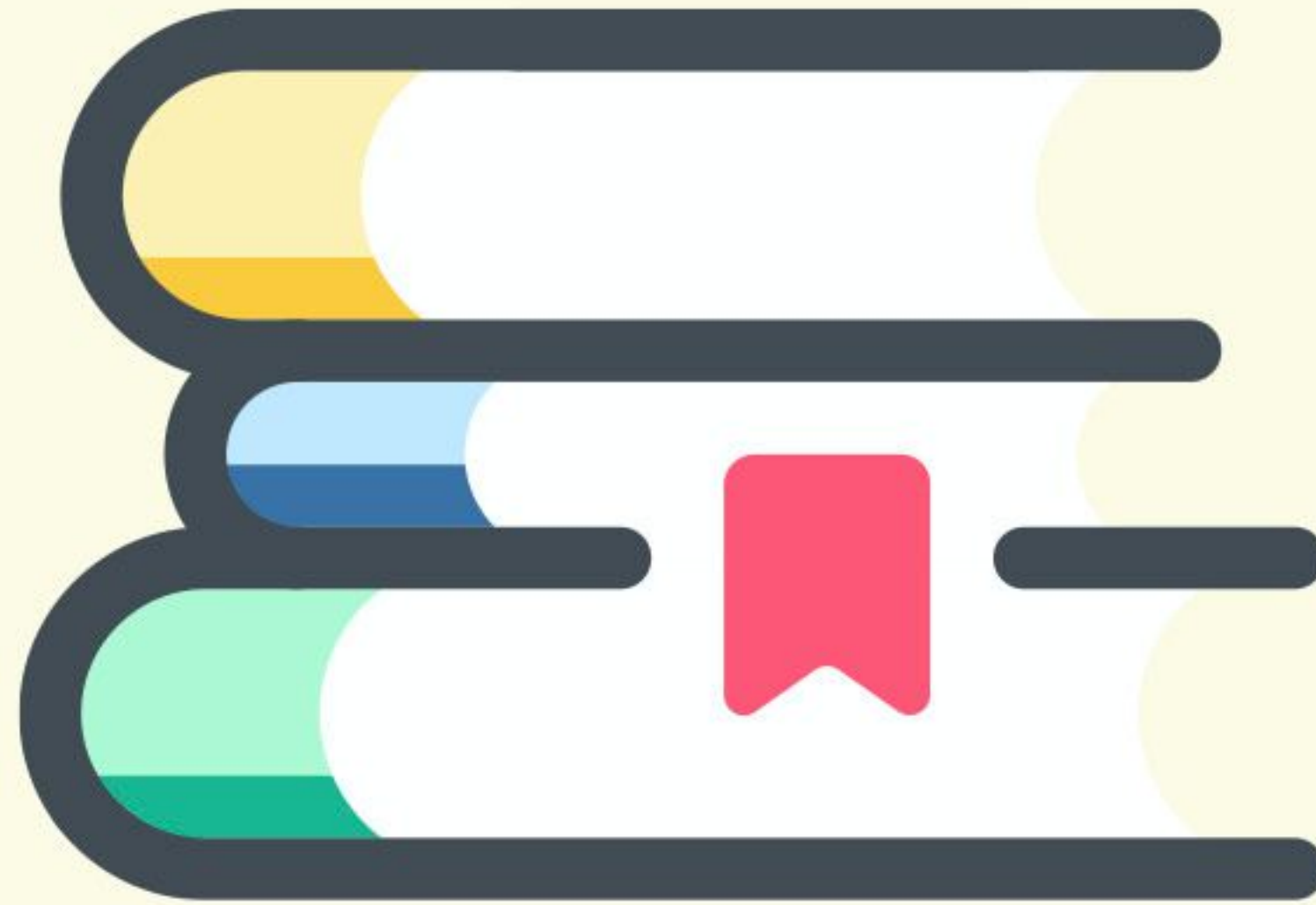


↓  
**Is that too risky?**

↓  
*Gather data & review*



↓  
**Apply mitigations**



# ISO/IEC 27001

**(Accepted standard for Information  
Security Management)**



# Risk Frameworks

**NIST 800-30**

**TRAI**

**STAMP**

**TOGAF**

**IEC 31010:2019**

**SMORS**

**STRIDE**

**DREAD**

**SABSA**



**All focus on impact**

# Data on Scope



**Industry  
Reports**

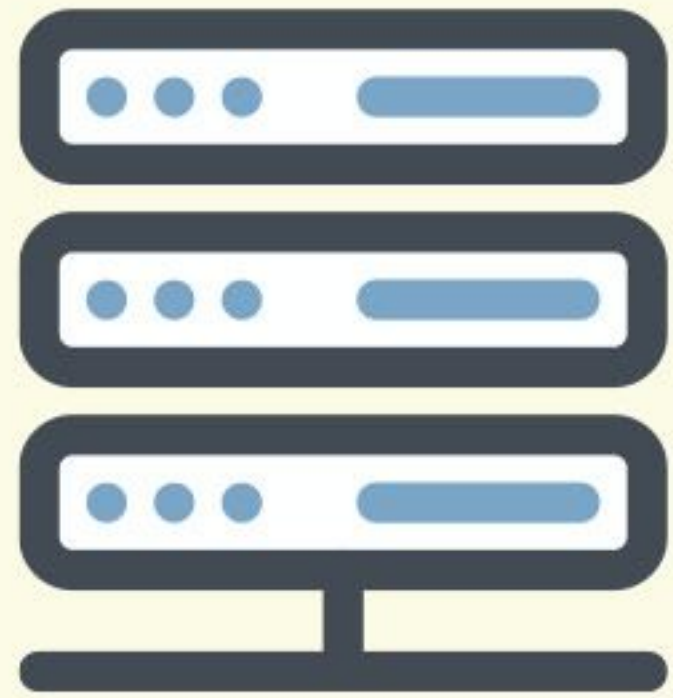


**Data Breach  
Reporting**



**Community  
Research**

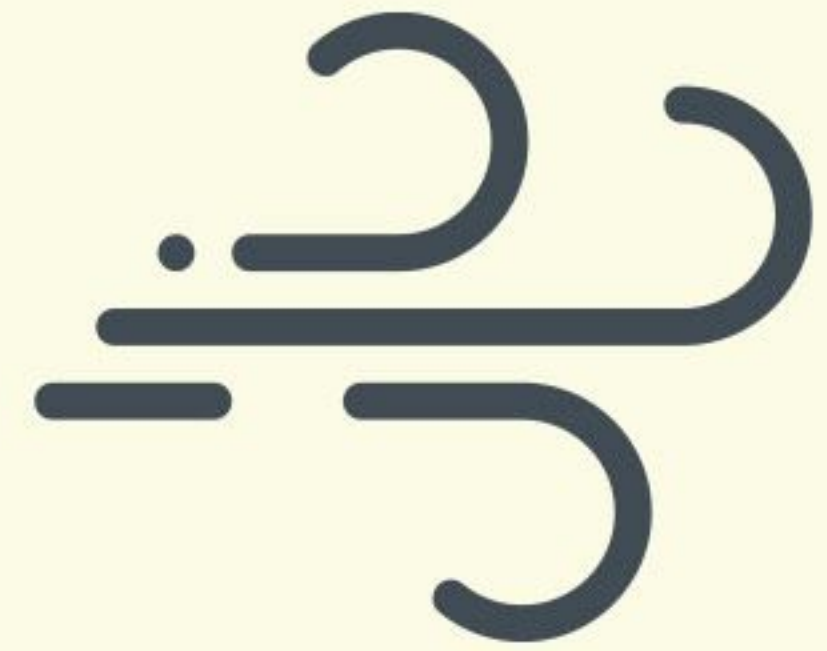
# Best Guess Scope



**# of Systems  
Affected**



**Data at  
Risk**



**Way the Wind  
is Blowing**

# Decision Workflow



**Impact of the event**



Attack gains control of system



*Gather data & review*



Data is important to org



**Likelihood it occurs**



Best guess: high/med/low



*Gather data & review*



**Is that too risky?**



*Gather data & review*



**Apply mitigations**





# Dealing With Risk



**Risk is a function of impact and likelihood**



**Gather as much data as possible**



**Make a reasonable decision**



**Monitor and iterate quickly**

# Thank You



**Mark Nunnikhoven**

Vice President, Cloud Research  
Trend Micro

@marknca | <https://markn.ca>