MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THE EVOLVING THREAT LANDSCAPE: FINDINGS FROM THE FRONT LINES

Cody Mercer

Threat Intelligence Security Analyst

Malwarebytes

AGENDA

- Cyber-Attack Trends 2017/2018 (Hardware & CPU)
- Threat & Vulnerability Management (TVM)
- Risk Management (RM) & Threat Modeling
- Protective Measures
- Key Takeaways

TOP MALWARE FAMILIES IN 2017/2018

01 Hijacker

02 Adware/Malvertising

03 Backdoor/APT’s

04 IOT/DDoS Attacks

05 Ransomware

06 Spyware

07 Cryptocurrency & Drive-By Mining

08 DDoS as Service/Ransomware as Service

09 Hardware Design Attack Vectors

COMPROMISED IOT DEVICES

Smart Cars
Drones

Cameras
Video Recorders

Televisions
Security Cameras
DVR’s

Gaming Platforms

HVAC Systems
Refrigerators
Electric Meters

Smart Phones
Watches

Pace Makers
Defibrillators
Insulin Pumps

HARDWARE ATTACKS

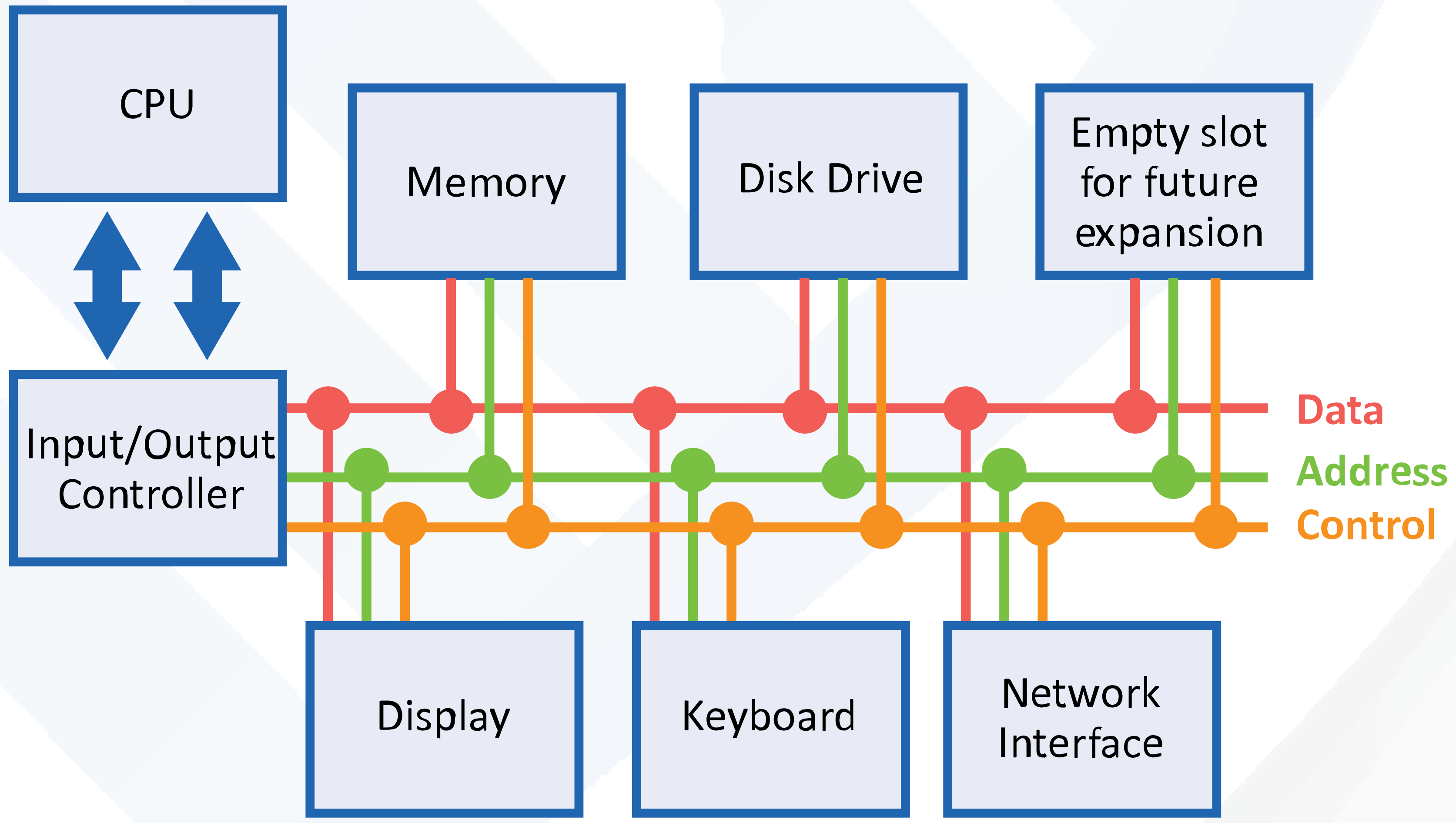
- Eavesdropping
- Inducing Disruptions
- Hardware Modification
- Backdoor Creation
- Counterfeiting Product Assets

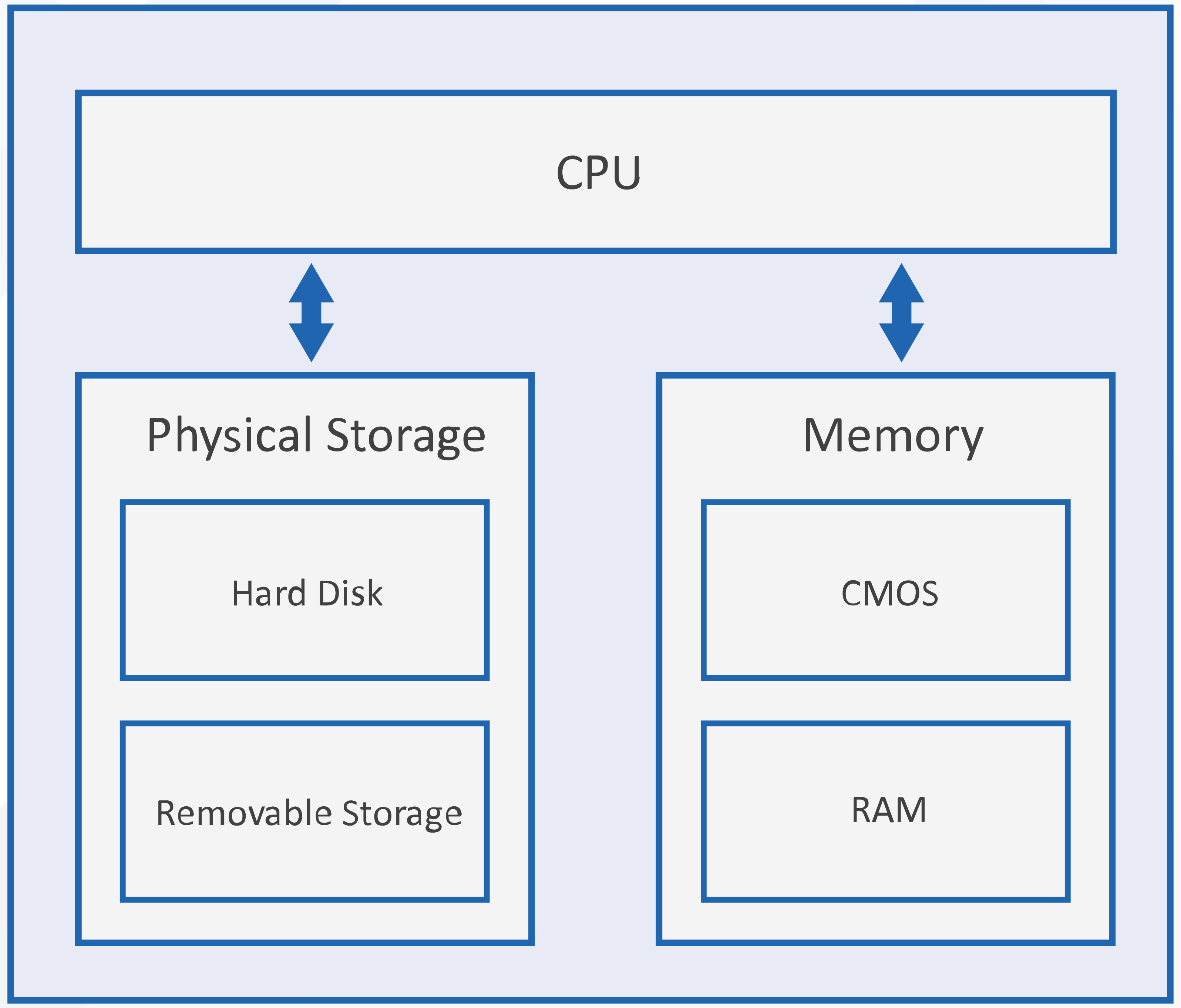
SPECTRE & MELTDOWN

- Permits access to “secured” kernel memory
- Windows, Linux, macOS, iOS, Android
- Spectre - Affects nearly all processors (AMD, Intel, ARM)
- Meltdown - Affects primarily Intel processors

SPECULATIVE EXECUTION

- Optimization technique used to determine where code is likely to go next to improve speed of asset.



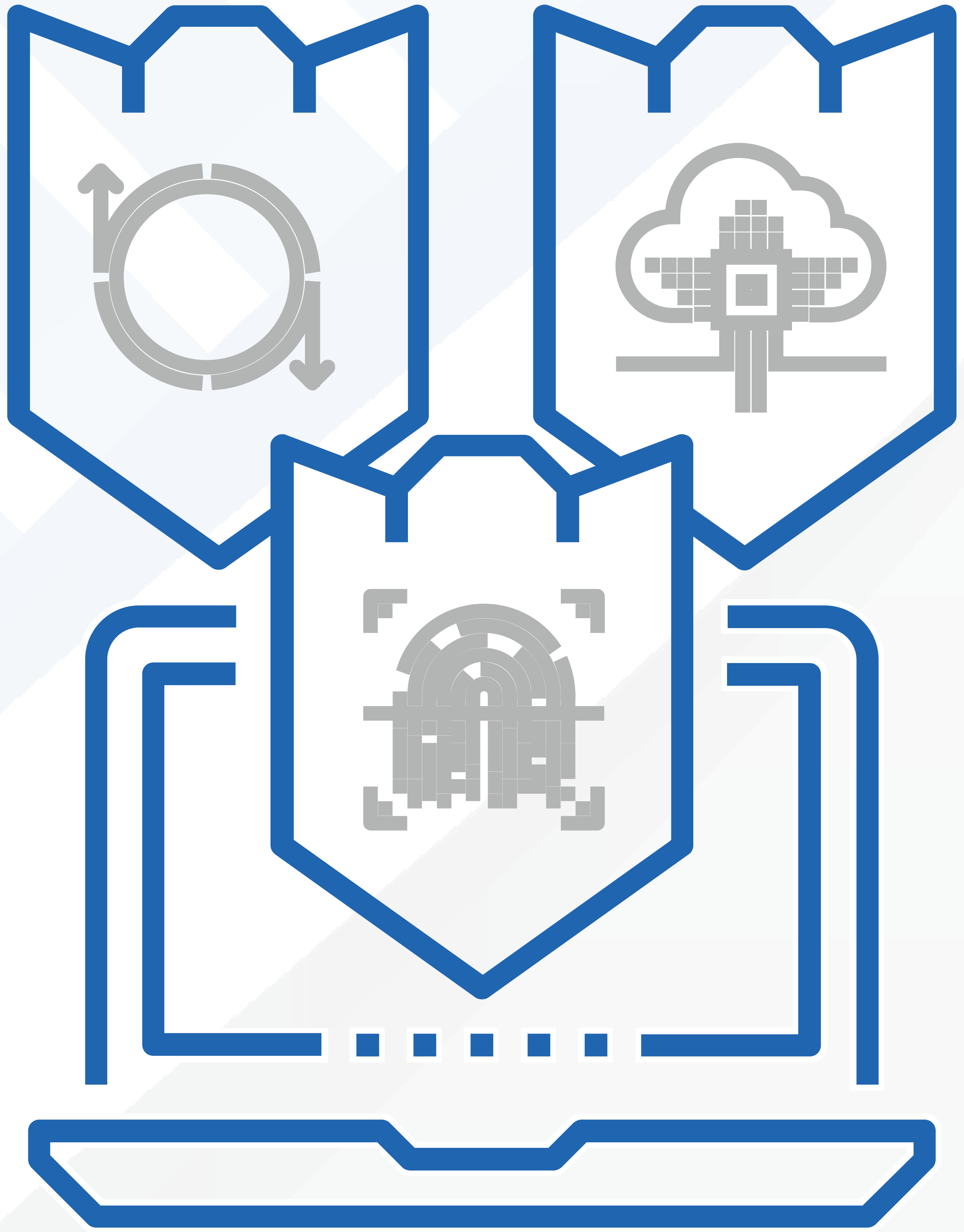


MEANS & MOTIVATIONS

- Disrupting services
- Imitating user authentication and elevation of privileges
- Data leakage
- Unlocking devices to gain access to kernel processing
- Unlocking hidden features

HARDWARE VULNERABILITY PROTECTION

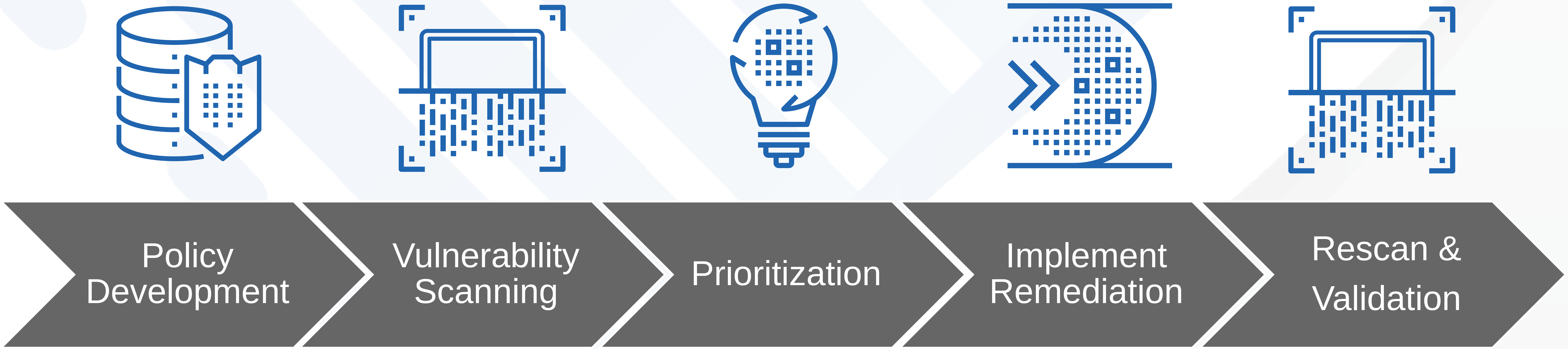
- Keep computer applications/firmware updated
- Vendor specific patches have been released and others are still in development
- May need complete re-development of the CPU architecture



InfoSecWorld Conference & Expo 2018

THREAT & VULNERABILITY MANAGEMENT (TVM)

THREAT & VULNERABILITY MANAGEMENT PROCESS



Policy Development

Vulnerability Scanning

Prioritization

Implement Remediation

Rescan & Validation

REASONS ORGANIZATIONS DON'T HAVE A TVM PROGRAM

- Lack of information security department or qualified personnel to apply patches
- No official enforcement or management of TVM program
- Testing/sandbox infrastructures are non-existent for patch review
- Formal approval needed for scanning delays process
- No budget

CONSEQUENCES OF NOT HAVING A TVM PROGRAM

Disrupted Business Process

Reputation & Branding Impact

Lost Operational Man-hours

Legal Penalties/ Enforcement Cost

Regulatory Risk

HIPAA

SOX

PCI

Theft of Data

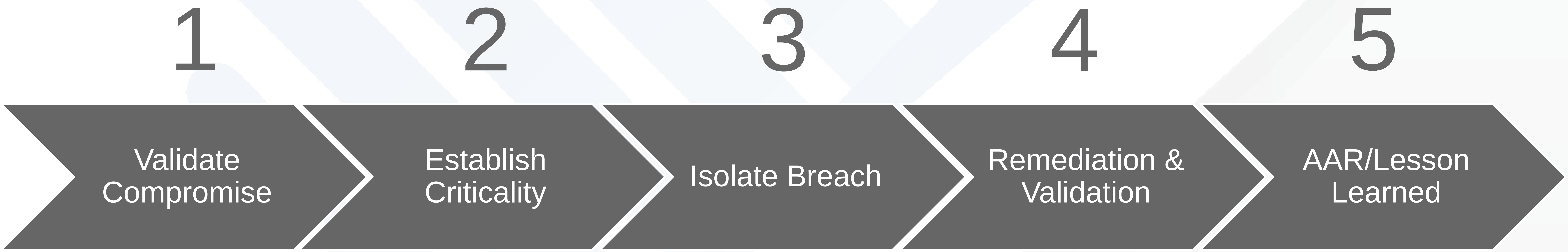
WHAT HAPPENS IF A PATCH DOESN'T EXIST

- Scans still need to be conducted to identify vulnerable assets
- Evaluate risk and apply a RM matrix for mitigation purposes
- Determine if the compromised asset will disrupt customer/business processes

!

TVM is a crucial part of security protection to any organization

REQUIRED TRIAGE PRACTICES



1 Validate Compromise

2 Establish Criticality

3 Isolate Breach

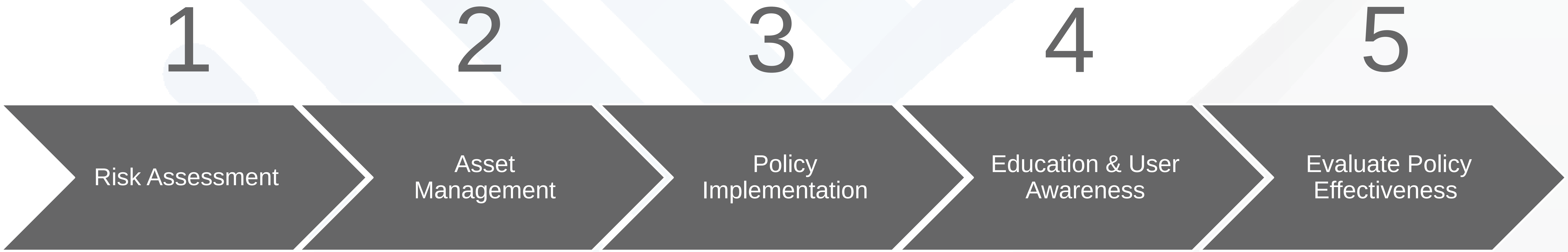
4 Remediation & Validation

5 AAR/Lesson Learned

RISK MANAGEMENT (RM)

THREAT MODELING

RISK MANAGEMENT PRINCIPALS



1 Risk Assessment

2 Asset Management

3 Policy Implementation

4 Education & User Awareness

5 Evaluate Policy Effectiveness

RISK EQUATION & THREAT MODELING

Risk

- Business disruption
- Financial losses
- Loss of privacy
- Damage to reputation
- Loss of confidence
- Legal penalties
- Impaired growth
- Loss of life

=

Threats

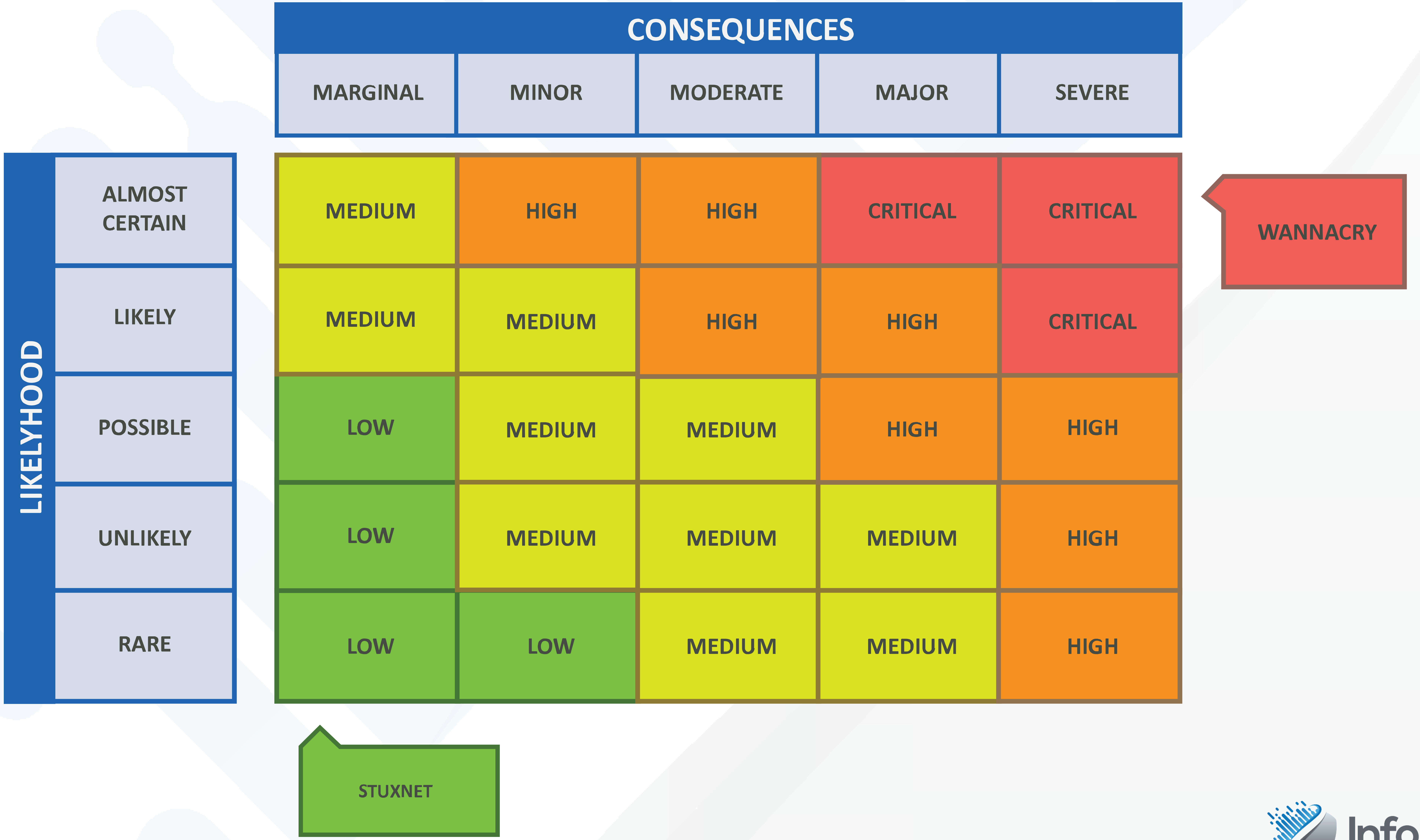
- Employees
- Contractors
- Criminals
- Governments
- Terrorists
- Competitors
- Hackers
- Nature

X

Vulnerabilities

- Software bugs
- Broken processes
- Ineffective controls
- Hardware flaws
- Business change
- Legacy systems
- Inadequate BCP
- Human error

RISK MATRIX & THREAT MODELING



		CONSEQUENCES				
		MARGINAL	MINOR	MODERATE	MAJOR	SEVERE
LIKELYHOOD	ALMOST CERTAIN	MEDIUM	HIGH	HIGH	CRITICAL	CRITICAL
	LIKELY	MEDIUM	MEDIUM	HIGH	HIGH	CRITICAL
	POSSIBLE	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	UNLIKELY	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
	RARE	LOW	LOW	MEDIUM	MEDIUM	HIGH

WANNACRY

STUXNET

BASIC SECURITY PRACTICES

Change/Configuration Management

Ransomware

Training/User Awareness

Network Security

Threat & Vulnerability Management

Security Solutions

KEY TAKEAWAYS

- Hardware attack-vectors are the next greatest threat surpassing that of any software vulnerability
- A TVM & RM program should be employed w/ threat modeling & risk matrix
- Basic security practices should be enforced to help facilitate protection

MIS|TI™ PRESENTS

InfoSecWorld

Conference & Expo 2018

THANK YOU

PLEASE FILL OUT YOUR EVALUATIONS!

Cody Mercer

Threat Intelligence Security Analyst

Malwarebytes