


# NIST Ransomware Workshop

## Status of NIST Ransomware Activities

Bill Fisher, Security Engineer, NCCoE

July 14, 2021

# Ransomware – Recent Times



“Ransomware as a threat  
has definitely become  
commoditized.”  
– Brian Krebs

## Escalating Impact

- Colonial Pipeline shut down for 6 days
- Kaseya event effected 1,500 organizations
- Washington DC police data leaked by ransomware group

## New Challenges

- Ransomware as a service (RaaS)
- Cryptocurrency payments
- Managed service providers are targets

## New Guidance

- Executive Order 14028 – NIST, DHS among other agencies called to charge.



# SP-1800 Data Security Portfolio



## › Data Integrity

- SP 1800-25 Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (ID-PR)
- SP 1800-26 Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events (DE-RS)
- SP 1800-11 Data Integrity: Recovering from Ransomware and Other Destructive Events (REC)



## > Data Confidentiality

- SP 1800-xx Data Confidentiality: Identifying and Protecting Assets Against and Data Against Data Breaches (ID-PR)
- SP 1800-xx Data Confidentiality: Detect, Respond to, and Recover from Data Breaches (DE-RS-RC)
- Both projects currently in build phase in the NCCoE lab. Project descriptions currently published



## > Data Availability Projected Work

- Given the overlap between Integrity, confidentiality and availability current plans are to release, for public comment, a white paper for data availability.






# Resources for Small Businesses





# Small Business Cybersecurity Corner



Search NIST

Menu

Information Technology Laboratory

SMALL BUSINESS CYBERSECURITY CORNER

Cybersecurity Basics

Planning Guides

Guidance by Topic

Responding to a Cyber Incident

Training

Partners

About & Contact Us

+

+

+


## Securing Data & Devices

*This page contains guidance to help you protect the security of your business information and devices (like cell phones and laptops).*

### TOPICS

<a href="#">Authentication</a>	<a href="#">Malware</a>	<a href="#">Privacy</a>
<a href="#">Data Protection</a>	<a href="#">Mobile Devices</a>	<a href="#">Securing a New Computer</a>
<a href="#">Denial of Service</a>	<a href="#">Phishing, Email, and Social Engineering</a>	<a href="#">Software &amp; Applications</a>
<a href="#">Internet of Things</a>	<a href="#">Physical Security</a>	<a href="#">Web and Social Networking</a>

CONNECT WITH US







# Important NIST Resources



# Ransomware Where Standards Help

## Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

### Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



NIST Special Publication 800-184

### Guide to Malware Prevention and Incident Response for Desktops

<http://dx.doi.org/10.6028/NIST.SP.800-184>

COMPUTER SECURITY

NIST Special Publication 800-184

### Guide for Enterprise Event Recovery

Michael Bartock  
Jeffrey Cichonski  
Mungliah Souppaya  
Matthew Smith  
Greg White  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-184>

SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

NIST Special Publication 800-46  
Revision 2

### Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Mungliah Souppaya  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-462>

COMPUTER SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# Ransomware Where Standards Help

**NIST Special Publication 800-83  
Revision 1**

## **Guide to Malware Incident Prevention and Handling for Desktops and Laptops**

Murugiah Souppaya  
Karen Scarfone

<http://dx.doi.org/10.6028/NIST.SP.800-83r1>

**COMPUTER SECURITY**

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

### **Framework for Improving Critical Infrastructure Cybersecurity**

Version 1.1

National Institute of Standards and Technology

April 16, 2018



NIST Special

### **Guide to Malware Prevention and Handling for Desktops and Laptops**

<http://dx.doi.org/10.6028/NIST.SP.800-83r1>

**COMPUTER SECURITY**

NIST Special Publication 800-184

### **Guide for Security Event Recovery**

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
Matthew Smith  
Greg Witte  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-184>

**COMPUTER SECURITY**

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

NIST Special Publication 800-46  
Revision 2

### **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security**

Murugiah Souppaya  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-46r2>

**COMPUTER SECURITY**

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

NIST Special Publication 800-40  
Revision 3

## Guide to Enterprise Patch Management Technologies

Murugiah Souppaya  
Karen Scarfone

<http://dx.doi.org/10.6028/NIST.SP.800-40r3>

COMPUTER SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Revision 4 in the works

Where  
T Docume

NIST SPECIAL PUBLICATION 1800-31A

## Improving Enterprise Patching for General IT Systems

Utilizing Existing Tools and Performing Processes in  
Better Ways

Volume A:  
Executive Summary

**Murugiah Souppaya**  
**Kevin Stine**  
National Cybersecurity Center of Excellence  
Information Technology Laboratory

**Mark Simos**  
**Sean Sweeney**  
Microsoft  
Redmond, Washington

**Karen Scarfone**  
Scarfone Cybersecurity  
Clifton, Virginia

September 2020

PRELIMINARY DRAFT

This publication is available free of charge from  
<https://www.nccoe.nist.gov/projects/building-blocks/patching-enterprise>

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

**NCCOE**  
NATIONAL CYBERSECURITY  
CENTER OF EXCELLENCE

Part B and C Preliminary draft target release is August

n 800-46  
revision 2

etwork,  
r Own  
ecurity

ah Souppaya  
en Scarfone

charge from:  
SP 800-462

Y

**NIST**  
Institute of  
Technology  
of Commerce

# Ransom Waiver Standards Help

NIST Special Publication 800-184

## Guide for Cybersecurity Event Recovery

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
Matthew Smith  
Greg Witte  
Karen Scarfone

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-184>

COMPUTER SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

### Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



NIST Special

### Guide to Managing Prevention and Detection

COMPUTER SECURITY

NIST Special Publication 800-184

### Guide for Cybersecurity Event Recovery

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
Matthew Smith  
Greg Witte  
Karen Scarfone

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-184>

COMPUTER SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

NIST Special Publication 800-46  
Revision 2

### Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-462>

COMPUTER SECURITY

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# Ransomware What Standards Help

NIST Special Publication 800-46  
Revision 2

## Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-46r2>

C O M P U T E R   S E C U R I T Y

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

Revision 3 in Progress – call for papers completed

### Framework for Improving Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018



NIST Special

### Guide to Malware Prevention and Desktop

<http://dx.doi.org/10.6028/NIST.SP.800-184>

C O M P U T E R   S

Special Publication 800-184

### Guide for Incident Event Recovery

Michael Bartock  
Jeffrey Cichonski  
Murugiah Souppaya  
Matthew Smith  
Greg Witte  
Karen Scarfone

This publication is available free of charge from:  
<https://doi.org/10.6028/NIST.SP.800-184>

S E C U R I T Y

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

NIST Special Publication 800-46  
Revision 2

### Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security

Murugiah Souppaya  
Karen Scarfone

This publication is available free of charge from:  
<http://dx.doi.org/10.6028/NIST.SP.800-46r2>

C O M P U T E R   S E C U R I T Y

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce



# New Cybersecurity Framework Profile





# New CSF Profile – Ransomware Risk Management

Preliminary Draft NISTIR 8374

## Cybersecurity Framework Profile for Ransomware Risk Management

William C. Barker  
Karen Scarfone  
William Fisher  
Murugiah Souppaya

---

*This is Preliminary Draft publication.  
For additional details, see the [Note to Reviewers](#) on page ii.*

---

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

- “Preliminary Draft” – comments closed 7/9. Document to be updated post Ransomware workshop. Next publication will be “Draft”
- Document maps CSF categories and informative references (such as NIST SP 800-53) to ransomware risk activities.
- Additional comments can be sent to [ransomware@nist.gov](mailto:ransomware@nist.gov)

# Ransomware Profile – Example

Category	Subcategory and Selected Informative References	Ransomware Application
<b>Risk Assessment (ID.RA):</b> The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	<b>ID.RA-1:</b> Asset vulnerabilities are identified and documented  <b>ISO/IEC 27001:2013</b> A.12.6.1, A.18.2.3  <b>NIST SP 800-53 Rev. 5</b> CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	Identifying and documenting the vulnerabilities of the organization's assets supports developing plans for and prioritizing the mitigation or elimination of those vulnerabilities, as well as contingency planning for evaluating and responding to future ransomware events. This will reduce the likelihood of a ransomware outbreak.
	<b>ID.RA-4:</b> Potential business impacts and likelihoods are identified  <b>ISO/IEC 27001:2013</b> A.16.1.6, Clause 6.1.2  <b>NIST SP 800-53 Rev. 5</b> RA-2, RA-3, SA-20, PM-9, PM-11	Understanding the business impacts of potential ransomware events is needed to support cybersecurity cost-benefit analyses as well to establish priorities for activities included in ransomware contingency plans for response and recovery. Understanding the potential business impacts also supports emergency response decisions in the event of a ransomware attack.
	<b>ID.RA-6:</b> Risk responses are identified and prioritized  <b>ISO/IEC 27001:2013</b> Clause 6.1.3  <b>NIST SP 800-53 Rev. 5</b> PM-4, PM-9	The expense associated with response to and recovery from ransomware events is materially affected by the effectiveness of contingency planning of responses to projected risks.

# > Contact Us



For more ransomware related NIST resources:

<https://csrc.nist.gov/Projects/ransomware-protection-and-response>

Contact us: Ransomware@nist.gov



<http://nccoe.nist.gov>



301-975-0200



[nccoe@nist.gov](mailto:nccoe@nist.gov)