The Impacts of Cyber Insurance on The Defense Industrial Base

Discussion of cyber insurance and the very real threats that contractors are facing as it relates to security standards such as NIST 800-171 and CMMC 2.0.

May 4th, 2022

Agenda

1. **Industry Overview**

   *Insights from Bob & Scott

2. **Connecting the dots between CMMC and NIST CSF**
3. **Takeaways & Next Steps**

SUMMIT7

Industry Overview

“Average total cost of a data breach increased by the largest margin in seven years.”

IBM Security

Cost of a Data Breach Report 2021

IBM

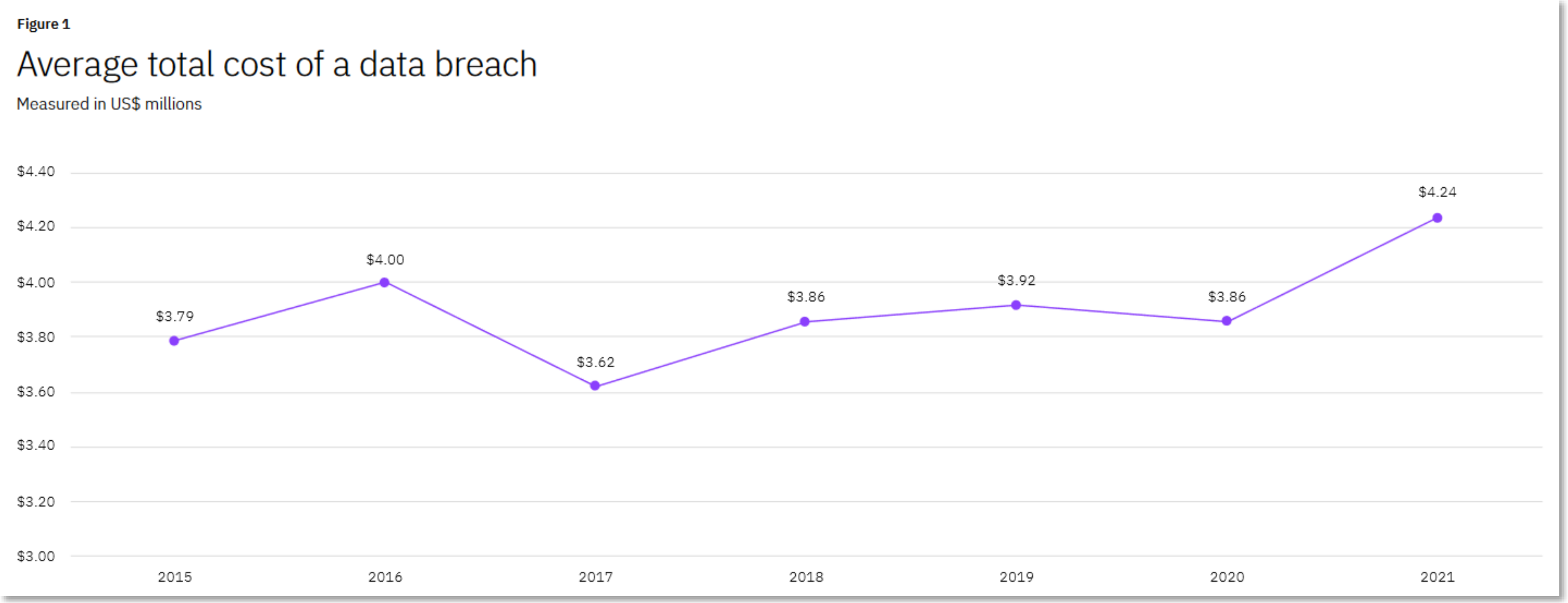


Figure 1

Average total cost of a data breach

Measured in US$ millions

“The cost of a data breach has increased by 11.9% since 2015”

“Lost business continued to represent the largest share of data breach costs for the seventh year in a row.”

IBM Security

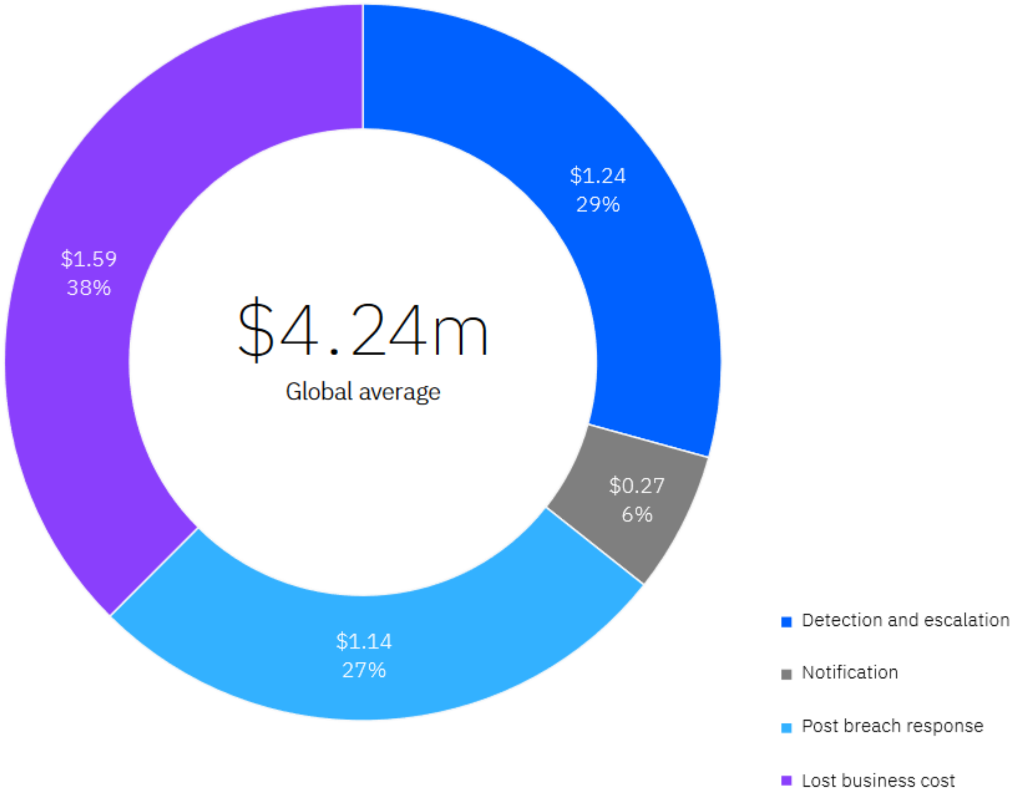
Cost of a Data Breach Report 2021

IBM

Figure 5

Average total cost of a data breach divided into four categories

Measured in US$ millions



“Data breach costs for small businesses increased 26.8% from 2020 to 2021.”

IBM Security

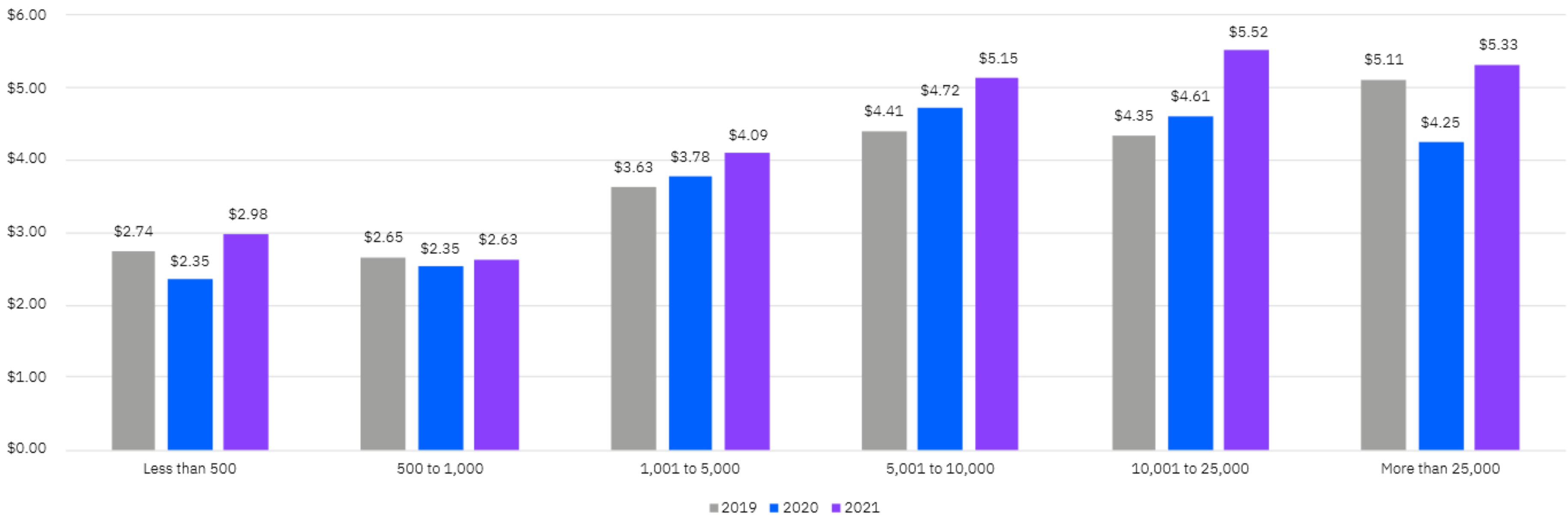
Cost of a Data Breach Report 2021

IBM

Figure 38

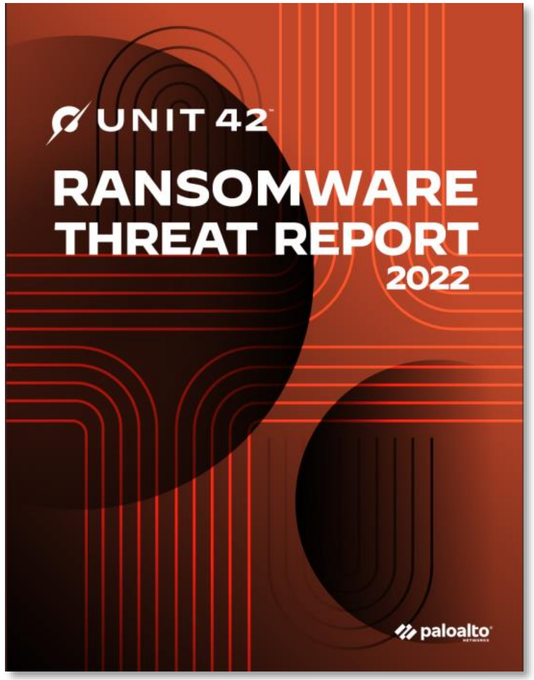
Average cost of a data breach by employee headcount

Measured in US$ millions



SUMMIT7

Average ransom payment rose 78% to $541,010 on cases worked by Unit 42 consultants

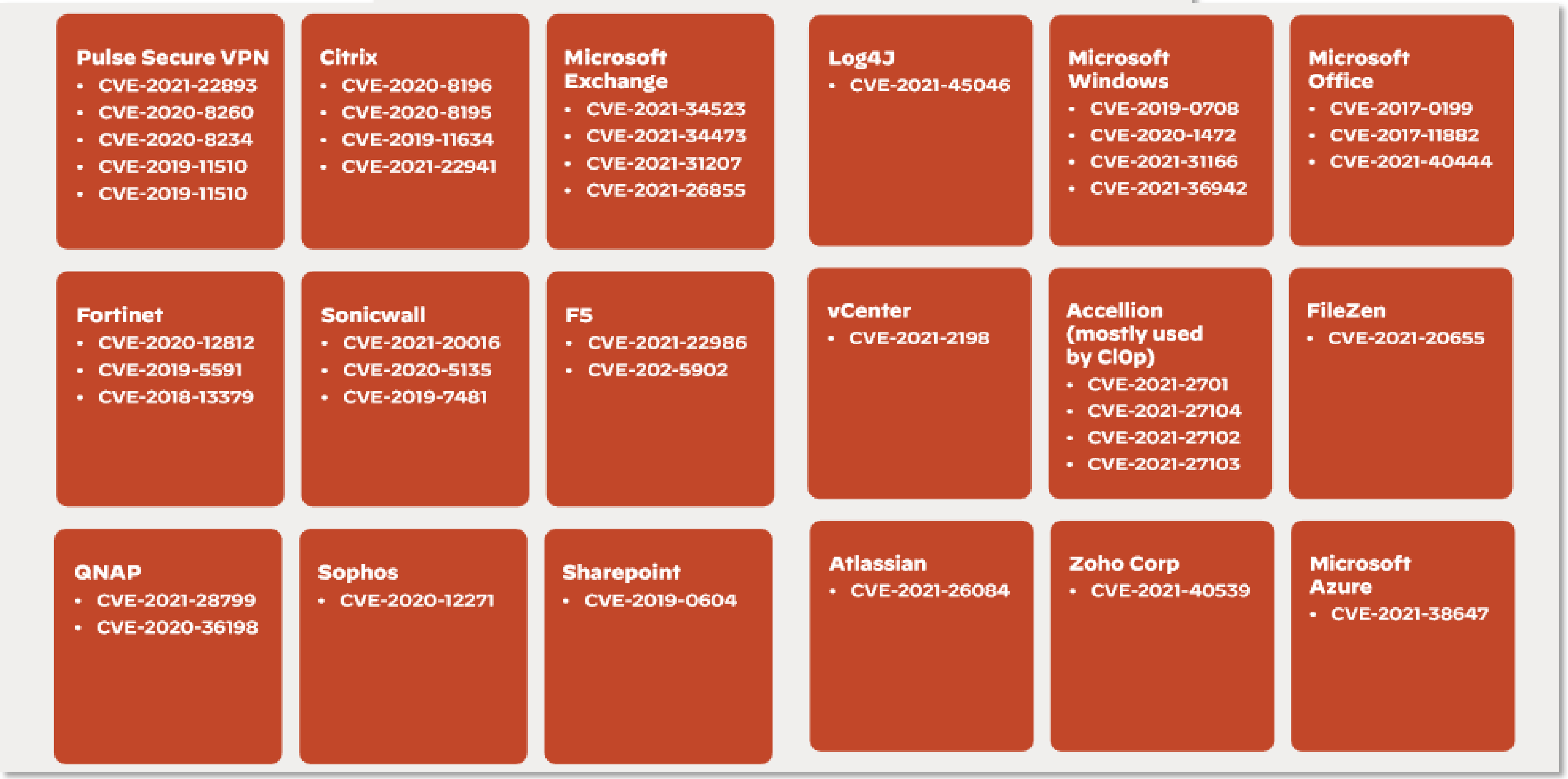


UNIT 42

RANSOMWARE THREAT REPORT 2022

paloalto

Figure 1: Vulnerabilities that have been observed being used by ransomware affiliates in 2021



Pulse Secure VPN
- CVE-2021-22893
- CVE-2020-8260
- CVE-2020-8234
- CVE-2019-11510
- CVE-2019-11510

Citrix
- CVE-2020-8196
- CVE-2020-8195
- CVE-2019-11634
- CVE-2021-22941

Microsoft Exchange
- CVE-2021-34523
- CVE-2021-34473
- CVE-2021-31207
- CVE-2021-26855

Log4J
- CVE-2021-45046

Microsoft Windows
- CVE-2019-0708
- CVE-2020-1472
- CVE-2021-31166
- CVE-2021-36942

Microsoft Office
- CVE-2017-0199
- CVE-2017-11882
- CVE-2021-40444

Fortinet
- CVE-2020-12812
- CVE-2019-5591
- CVE-2018-13379

Sonicwall
- CVE-2021-20016
- CVE-2020-5135
- CVE-2019-7481

F5
- CVE-2021-22986
- CVE-202-5902

vCenter
- CVE-2021-2198

Accellion (mostly used by Cl0p)
- CVE-2021-2701
- CVE-2021-27104
- CVE-2021-27102
- CVE-2021-27103

FileZen
- CVE-2021-20655

QNAP
- CVE-2021-28799
- CVE-2020-36198

Sophos
- CVE-2020-12271

Sharepoint
- CVE-2019-0604

Atlassian
- CVE-2021-26084

Zoho Corp
- CVE-2021-40539

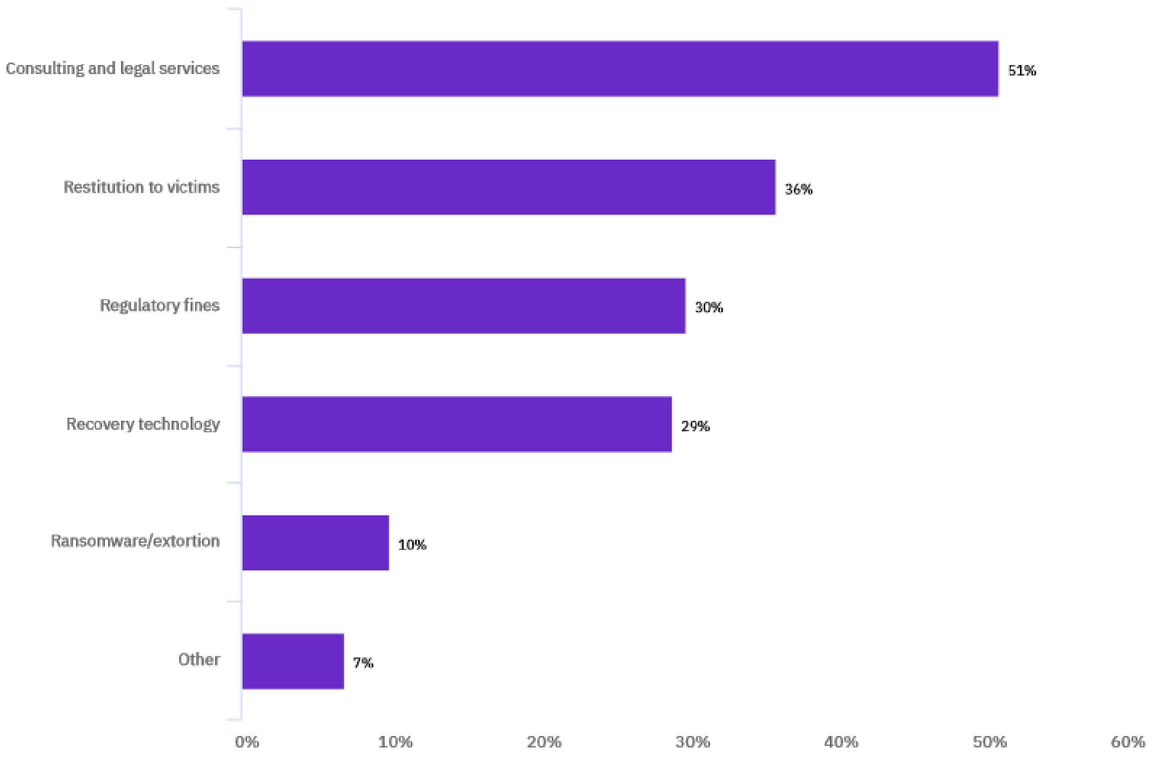
Microsoft Azure
- CVE-2021-38647

“Only 10% of organizations with cyber insurance used claims to cover the cost of ransomware or extortion.”

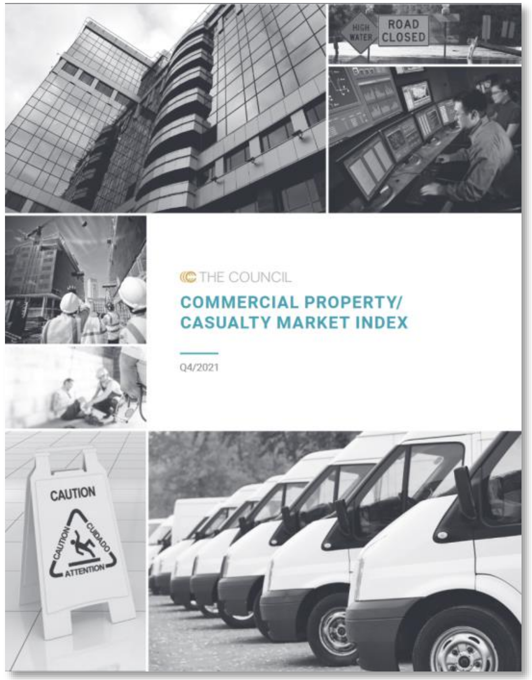
Figure 27

Types of costs recovered using cybersecurity insurance claims

Percentage of responses, more than one response allowed



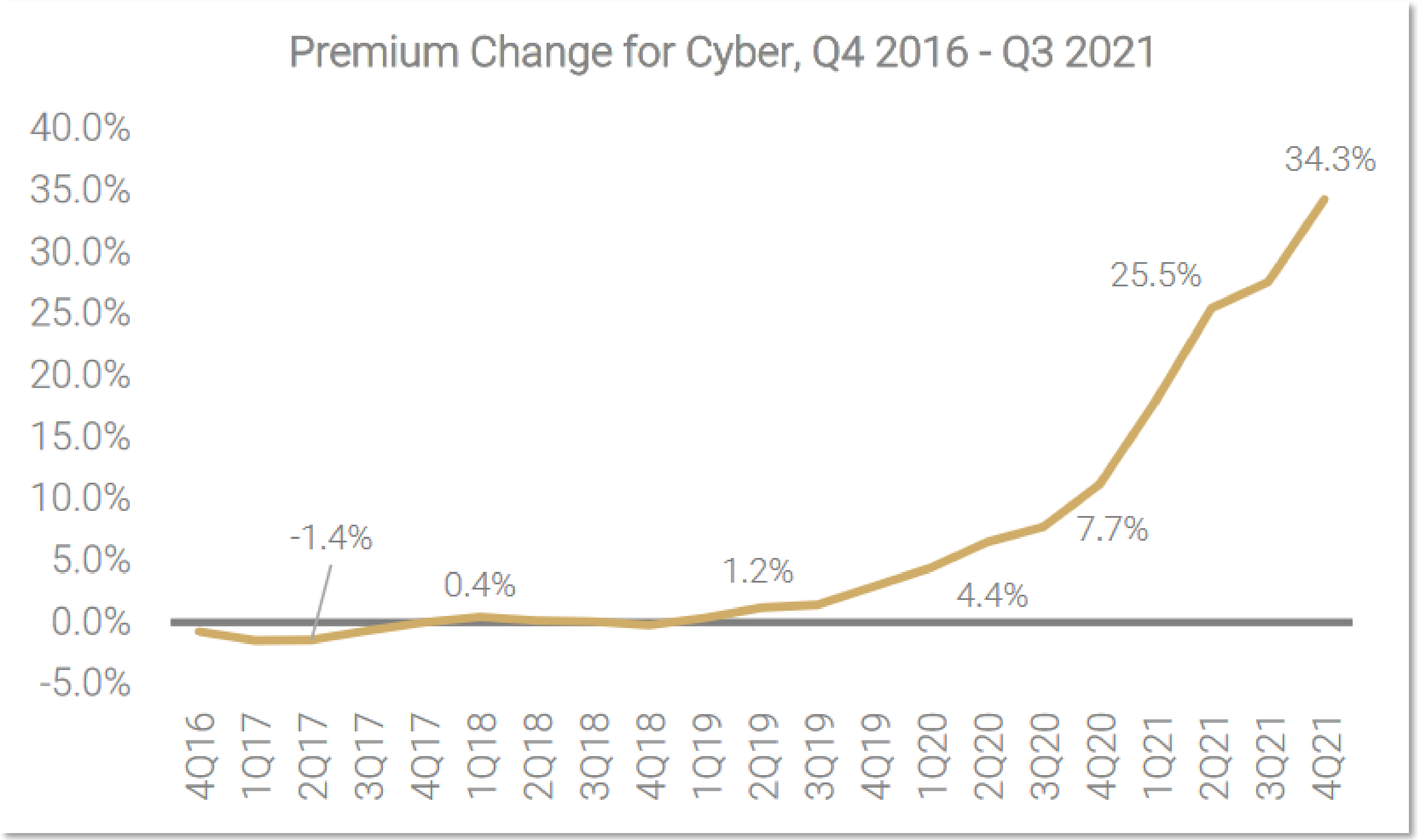
“Sophisticated bad actors targeted smaller firms with limited defenses and resources.”



THE COUNCIL

COMMERCIAL PROPERTY/ CASUALTY MARKET INDEX

Q4/2021



Premium Change for Cyber, Q4 2016 - Q3 2021

SUMMIT7

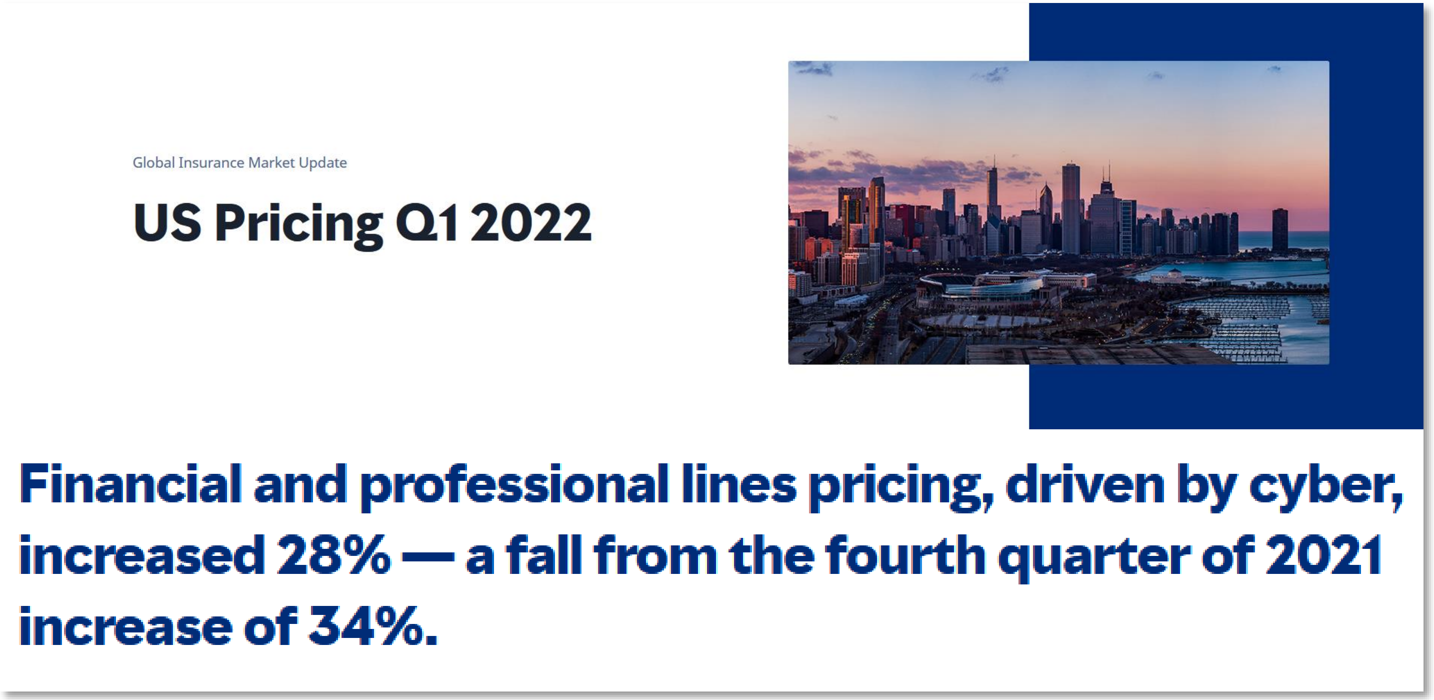
"Cyber underwriting continued to focus on a company's control environment and demonstrated cybersecurity maturity."

Marsh

Global insurance markets: Pricing increases moderate in 2021, with exception of cyber

- "Cyber remained the most challenging coverage area, driven by ransomware claims, with considerable pressure on pricing and deductibles, a reduction in capacity, and narrowing of key coverages."
- "Cyber pricing increased 130%, affected by the continued increase in the frequency and severity of ransomware claims."
- "Business interruption and data exfiltration contributed to the increasing total claim pay-outs from ransomware events."

“Cyber underwriting continued to focus on a company’s control environment and cybersecurity maturity.”



Global Insurance Market Update

US Pricing Q1 2022

Financial and professional lines pricing, driven by cyber, increased 28% — a fall from the fourth quarter of 2021 increase of 34%.

- “Cyber pricing increased 110%, in large part due to the re-pricing and re-underwriting of cyber risks.”
- “Heightened frequency and severity of claims activity contributed significantly to pricing increases.”
- “Over 60% of clients took higher retentions to help offset premium impact.”

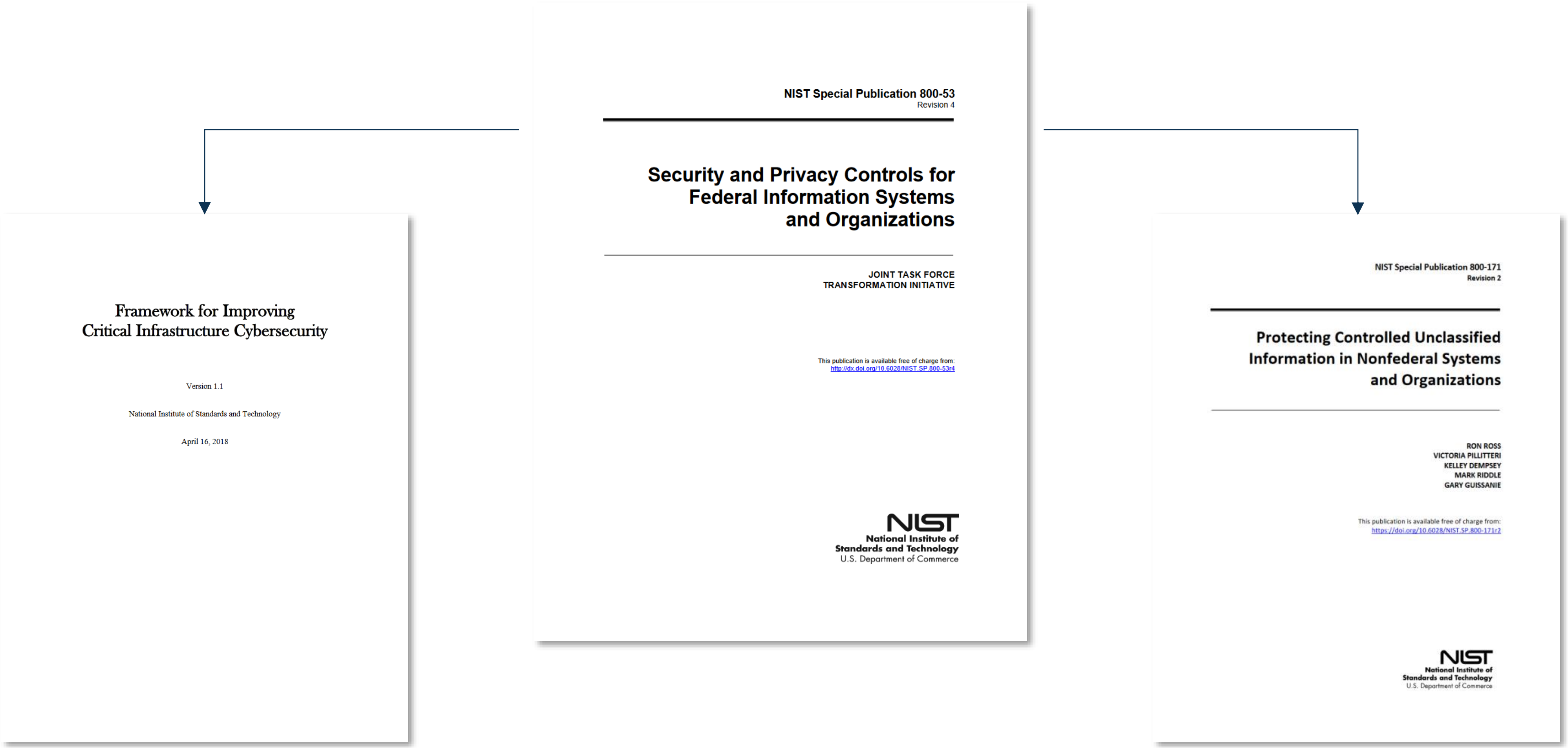
SUMMIT7

How CMMC Helps

Comparing NIST SP 800-171 to the NIST Ransomware Profile

SUMMIT7

The NIST Cybersecurity Framework (CSF) and NIST SP 800-171 are both derived from NIST SP 800-53.



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

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 Publication 800-171
Revision 2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

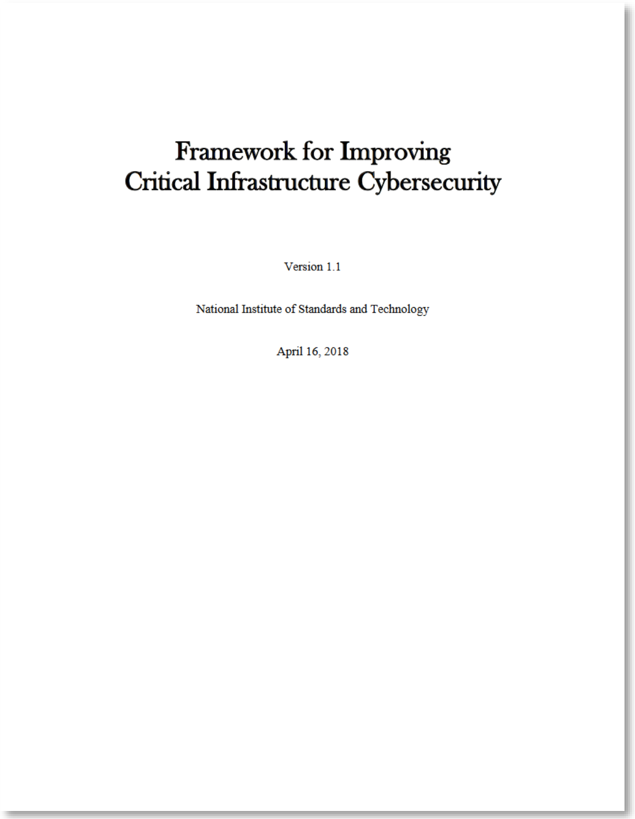
RON ROSS
VICTORIA PILLITTERI
KELLEY DEMPSEY
MARK RIDDLE
GARY GUISSANIE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r2

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

SUMMIT7

CSF “Functions” organize basic cyber activities at their highest level.



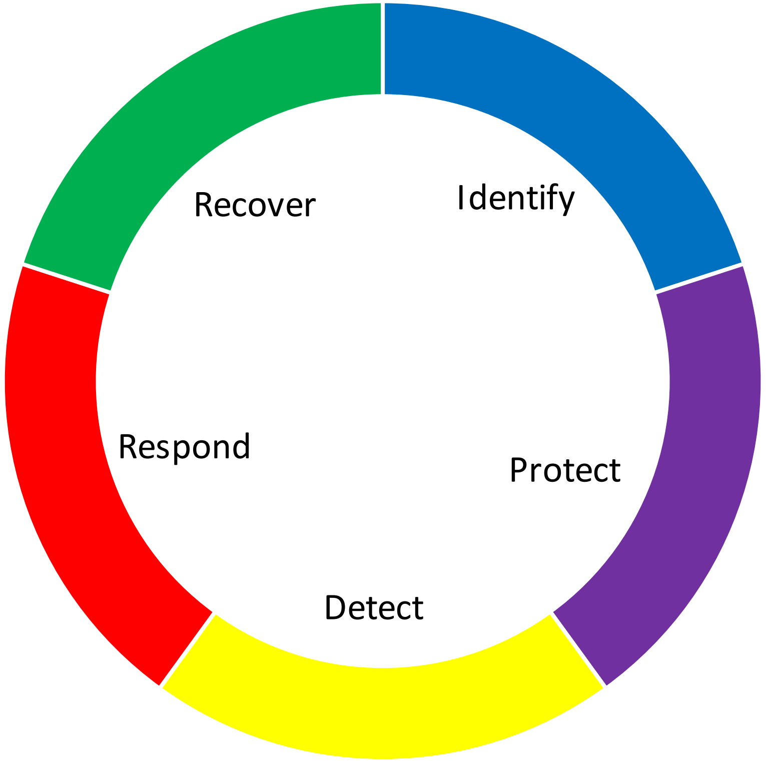
Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

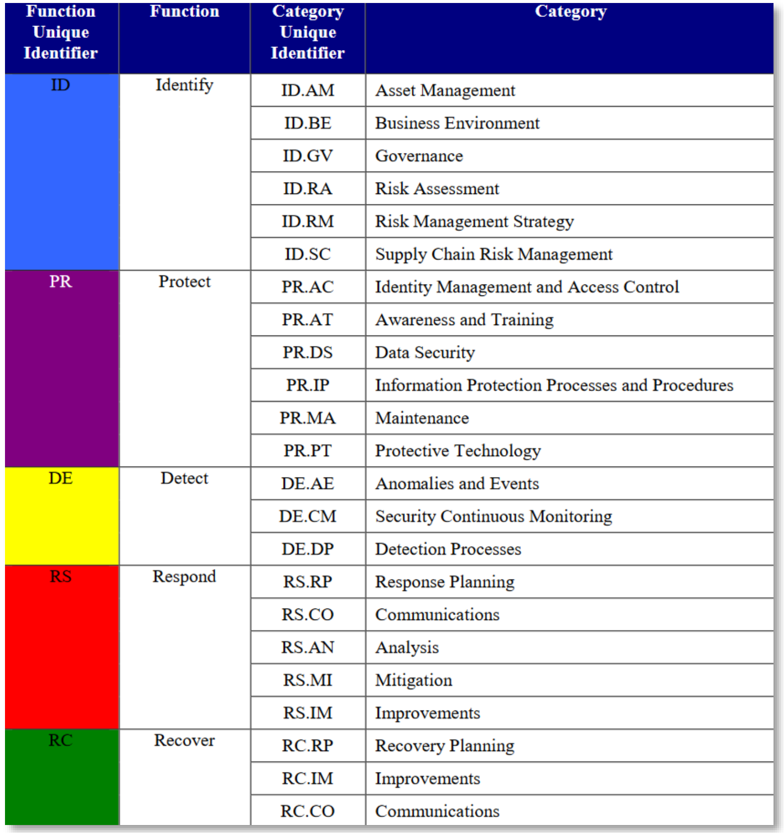
National Institute of Standards and Technology

April 16, 2018

Five Functions of the Framework “Core”

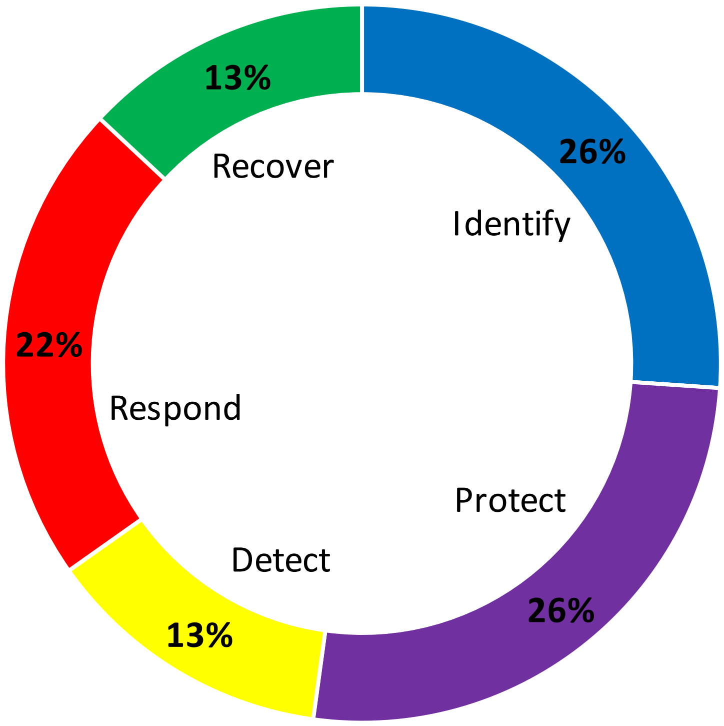


CSF Functions are subdivided into 23 “categories”

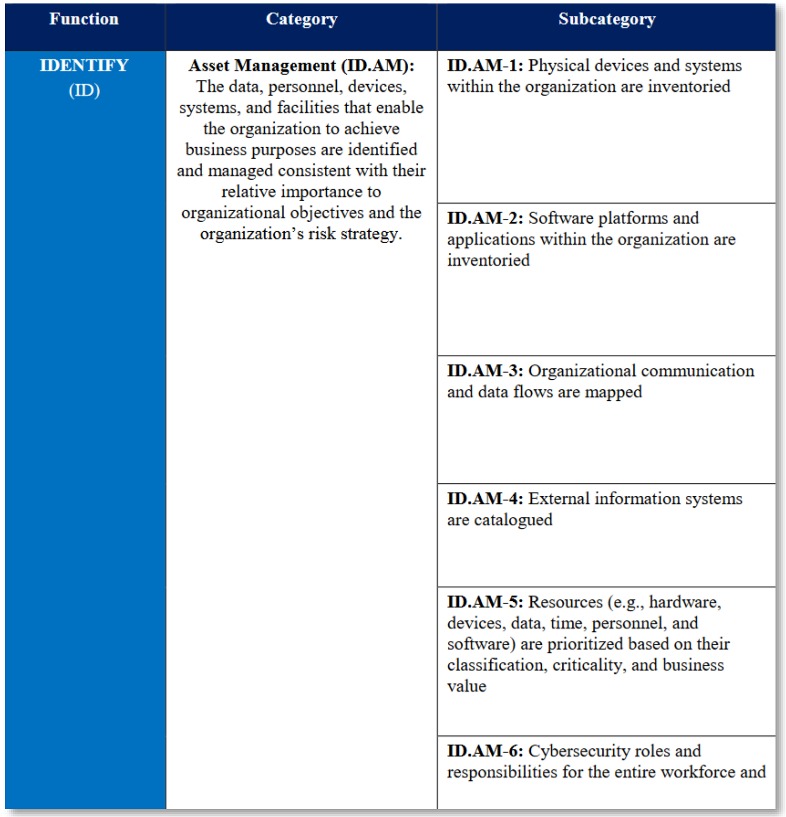


Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Core Functions by Category %

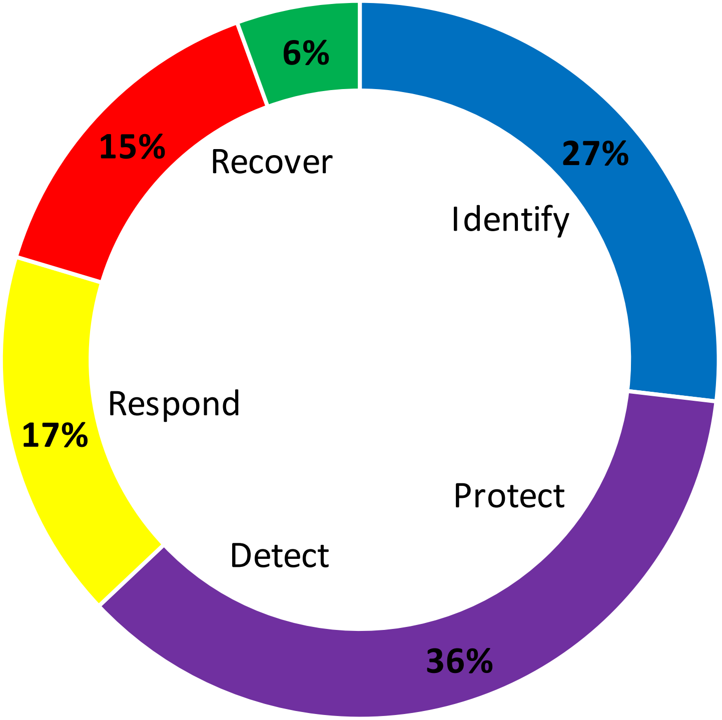


CSF categories are further subdivided into “subcategories”.

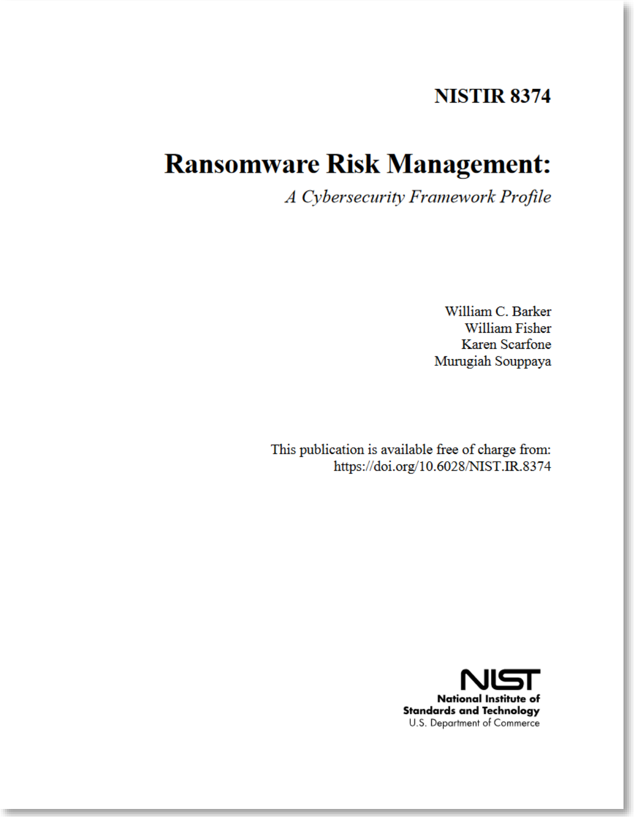


Function	Category	Subcategory
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization’s risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried
		ID.AM-2: Software platforms and applications within the organization are inventoried
		ID.AM-3: Organizational communication and data flows are mapped
		ID.AM-4: External information systems are catalogued
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and

Core Functions by Subcategory %



“Profiles” are a selection of CSF categories and subcategories that help gauge readiness.



NISTIR 8374

Ransomware Risk Management:

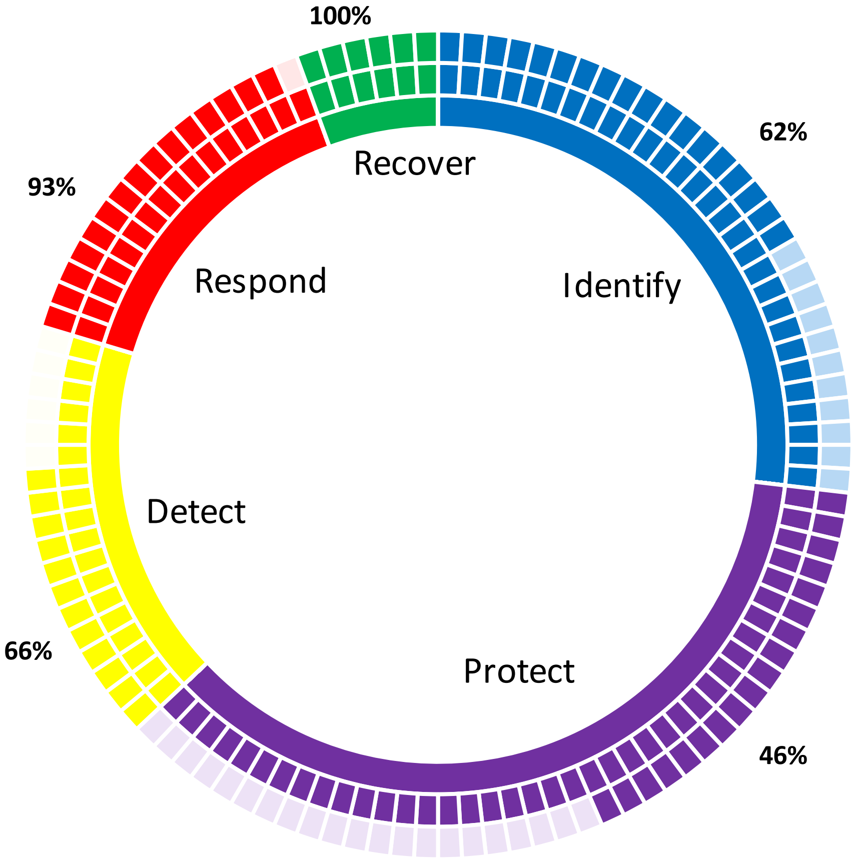
A Cybersecurity Framework Profile

William C. Barker
William Fisher
Karen Scarfone
Murugiah Souppaya

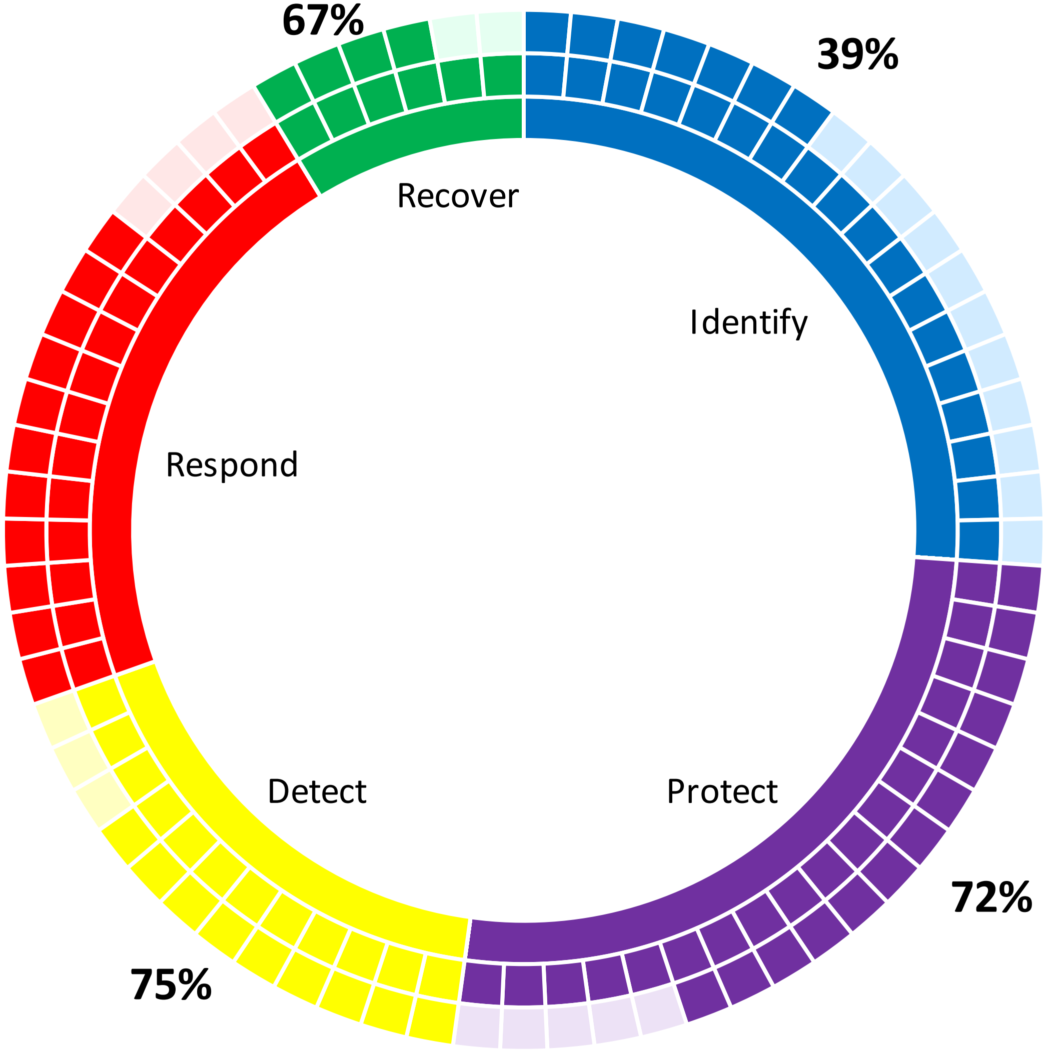
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8374

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

NIST Ransomware Profile by CSF Subcategory %



64% of the NIST Ransomware Profile is covered by NIST SP 800-171.



Key Takeaways & Next Steps

What should organizations do next?

Key Takeaways

- Cyber Insurance is harder to get

- Primes and other Customers are asking for more Cyber coverage

- Cyber Insurance costs are increasing

- Securing your systems to a defined standard may help lower underwriting costs

SUMMIT7

Q & A

Bob Metzger

Jacob Horne

Scott Edwards

SUMMIT7