Xceptional TechData CISCO Partner

Compliance Panel Discussion

Getting a Jump Start on CMMC

August 26, 2021

Agenda

- Panelist Introductions
- Conversation Set Up
- Impact of Compliance & Regulatory Actions
- Top Cyber Attacks, Trends
- Panel Questions
- Key Decisions, Options
- Drawing & Prizes!

Panelists

Mark Dallmeier, Xceptional

Vice President, CSO/CMO

Industry Researcher, Analyst

Mark is a Senior Executive, Serial Entrepreneur, CSO/CMO and Board Advisor for various companies who over the last 25 years has co-founded and grown companies in multiple industries. Previously Mark spent 5 years as the CSO/CMO at Terra Verde (now Avertium), an award-winning cybersecurity consultancy and MSSP. Prior to Avertium, Mark spent 5 years at IT Partners an award-winning data center solution provider and VAR, driving the company's transformation and portfolio expansion. Mark was the Chief Strategy / Marketing Officer and a Board Director at 3 Sigma Corporation, driving corporate-wide transformation and growth initiatives, accelerating double digit revenue growth and the commercialization of new products. As the President and CEO of The ROBB Group and co-founder of Channel Savvy (sold to Avnet), Mark consulted to early-stage hyper-growth companies and Fortune 100, driving sales and transformation and growth initiatives, deploying new sales-marketing-operations-service delivery best practices, generating over $1.8B in new revenue for those companies. Mark actively publishes research, speaks and facilitates workshops on corporate growth, cybersecurity, risk and transformation topics.

Don Maclean, DLT

Registered CMMC Practitioner, CISSP, Forrester ZTX Strategist & Chief Cyber Security Technologist

Certified as a CMMC Registered Practitioner, Don Maclean currently serves as DLT's Chief Cybersecurity Technologist. A recipient of the FedScoop 50 award and ICIT Fellow, Mr. Maclean's duties include formulating and executing cybersecurity portfolio strategy, speaking and writing on security topics, and socializing DLT's cybersecurity offerings. In this capacity, Mr. Maclean also advises CEOs on Federal go-to-market strategies for cybersecurity products. Before joining DLT in 2015, Mr. Maclean ran security programs for U.S. Federal agencies, including DOJ, DOL, FAA, FBI, and Treasury. This experience allowed him to observe the strengths and limitations of traditional cybersecurity defenses. Mr. Maclean is a Forrester Zero Trust eXtended (ZTX) Strategist and holds CISSP, CEH, AWS Certified Practitioner and CCSK certifications in addition to an M.S. in Information Security and a B.A. in Music. An avid musician, Don organizes a concert for charity every year, and often competes in chess and Shogi (Japanese chess) tournaments and has recently started building model ships while quarantined due to COVID.

Richard Lundy, Tech Data Government Solutions

Facility Security Officer

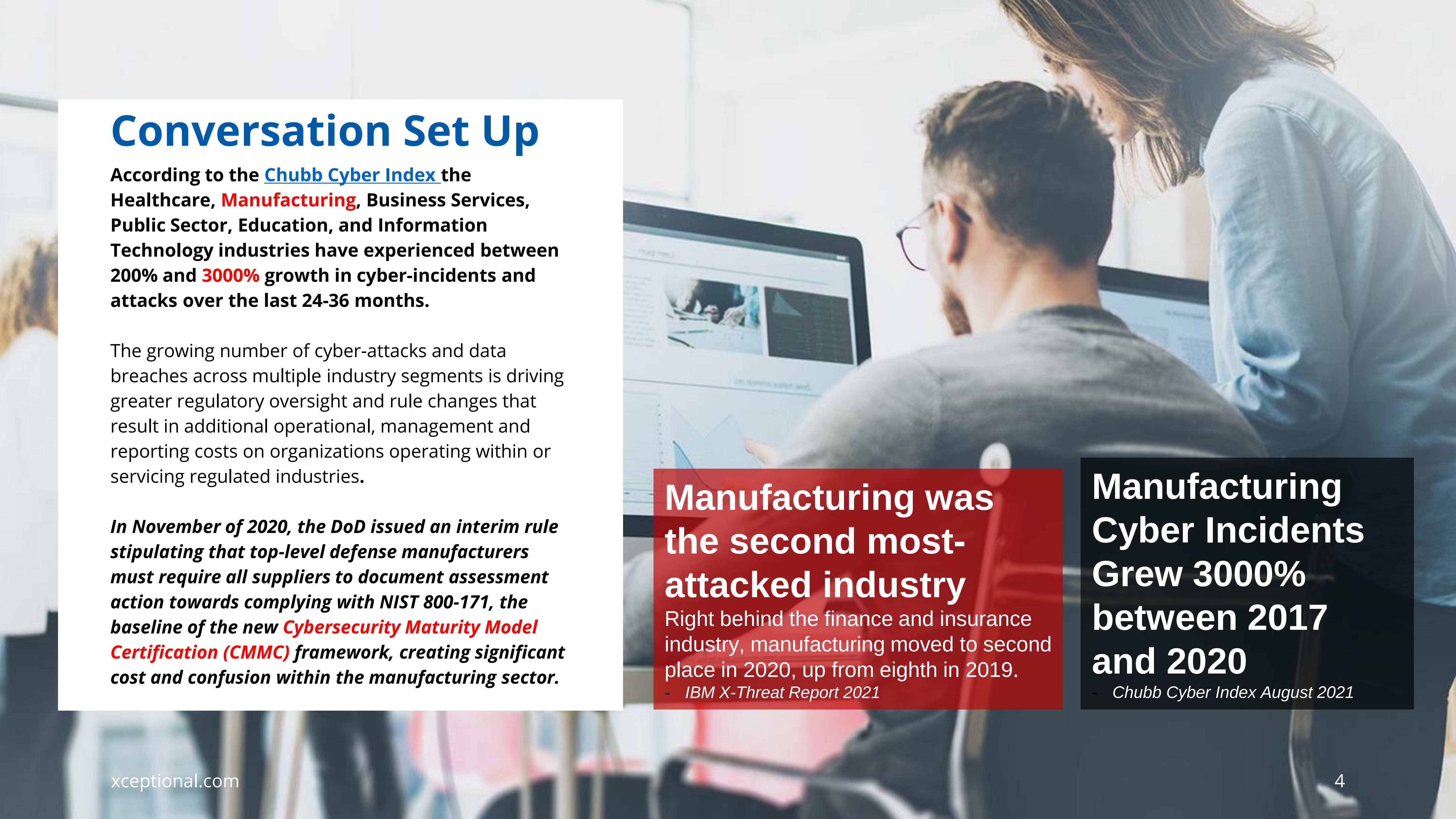
Richard Lundy serves as federal security program officer and provides security oversight for TD. Mr. Lundy also serves as Market Development Specialist with focus on federal system Integrators (FSI) working with intel customers, TD partners, vendors and internal resources in identifying, developing and advancing business in the Federal market. Previous to joining TDGS in 2014, Mr. Lundy served as Chief of Information Protection for the United States Air Force, 911th Airlift Wing where he provided program oversite across multiple security functions. His mission was to create a supportive environment for protecting information in order to conduct effective air, space and cyberspace operations. Mr. Lundy is a (RET) Chief Master Sergeant who last served as the Chief enlisted manager, Pittsburgh Air Reserve Base, PA. He represented the cradle to grave operations and services provided to the standing population of over 1500 hundred active, reserve and civilian personnel. He has taken on various positions throughout his career in human resources, career enhancement, readiness and as a Combat Controller executing key joint multi-national special operations capabilities with US allies and sister services across Pacific.

Drew Kaiser, Tech Data

Solutions Architect (Cisco)

Over the years, Drew has worked within the legal, medical, and hospitality verticals. The breadth of Drew's career has been customer facing within systems management, network engineering, and cybersecurity roles delivering project planning, deployment, and troubleshooting.

Drew's services have been aligned with vendors like Cisco, HP, Juniper, SonicWALL, Palo Alto, Fortinet, Microsoft Azure, VMware, and other cloud based appliances/services for compliancy, network optimization, and security. As a solution architect at Tech Data he is specialized in Cisco cybersecurity products, and has technical certifications ranging from Cisco specialized to vendor agnostic certifications like CISSP.



Conversation Set Up

According to the Chubb Cyber Index the Healthcare, Manufacturing, Business Services, Public Sector, Education, and Information Technology industries have experienced between 200% and 3000% growth in cyber-incidents and attacks over the last 24-36 months.

The growing number of cyber-attacks and data breaches across multiple industry segments is driving greater regulatory oversight and rule changes that result in additional operational, management and reporting costs on organizations operating within or servicing regulated industries.

In November of 2020, the DoD issued an interim rule stipulating that top-level defense manufacturers must require all suppliers to document assessment action towards complying with NIST 800-171, the baseline of the new Cybersecurity Maturity Model Certification (CMMC) framework, creating significant cost and confusion within the manufacturing sector.

Manufacturing was the second most-attacked industry

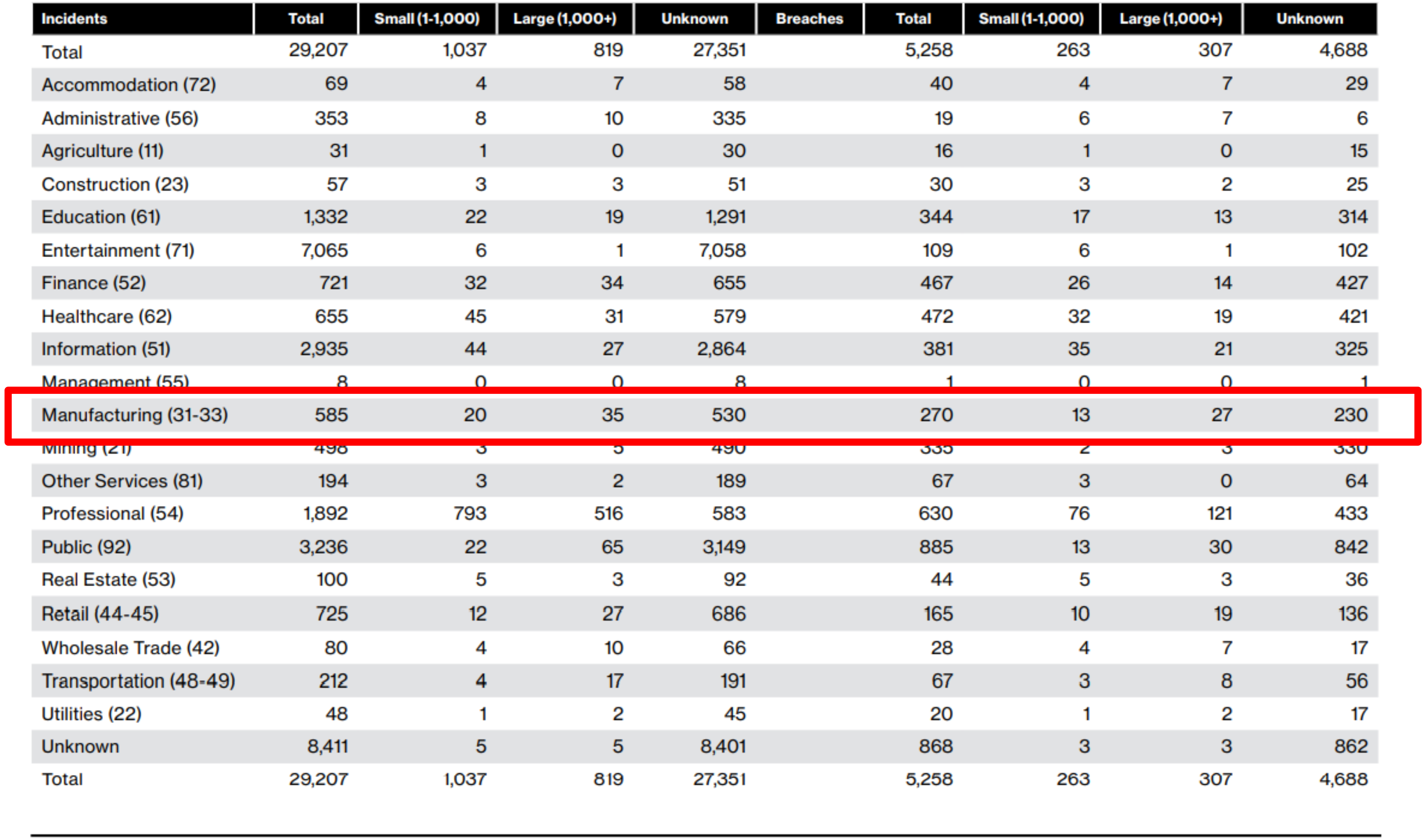
Right behind the finance and insurance industry, manufacturing moved to second place in 2020, up from eighth in 2019.

- *IBM X-Threat Report 2021*

Manufacturing Cyber Incidents Grew 3000% between 2017 and 2020

- *Chubb Cyber Index August 2021*

Top Industries Under Attack & Breached

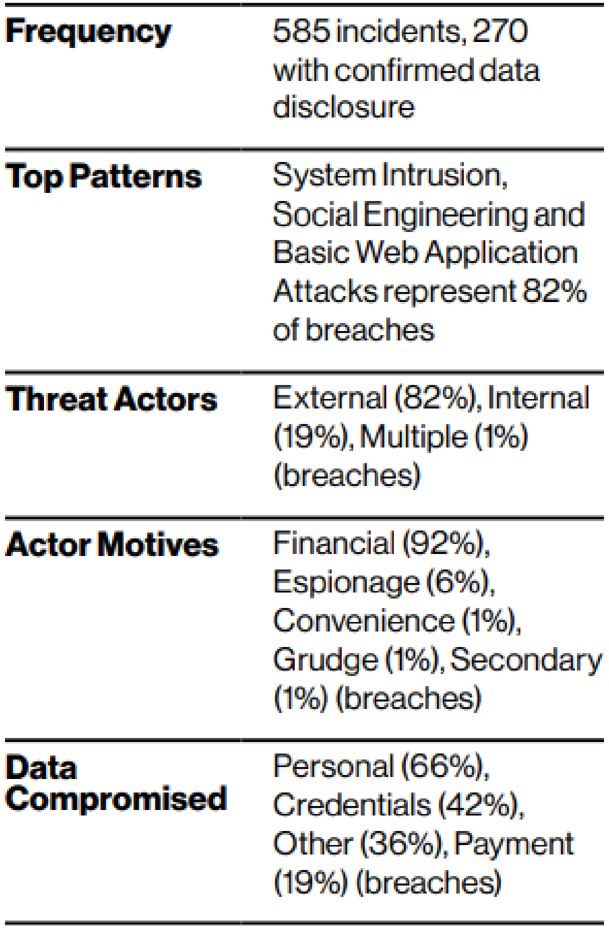


Incidents	Total	Small (1-1,000)	Large (1,000+)	Unknown	Breaches	Total	Small (1-1,000)	Large (1,000+)	Unknown
Total	29,207	1,037	819	27,351		5,258	263	307	4,688
Accommodation (72)	69	4	7	58		40	4	7	29
Administrative (56)	353	8	10	335		19	6	7	6
Agriculture (11)	31	1	0	30		16	1	0	15
Construction (23)	57	3	3	51		30	3	2	25
Education (61)	1,332	22	19	1,291		344	17	13	314
Entertainment (71)	7,065	6	1	7,058		109	6	1	102
Finance (52)	721	32	34	655		467	26	14	427
Healthcare (62)	655	45	31	579		472	32	19	421
Information (51)	2,935	44	27	2,864		381	35	21	325
Management (55)	8	0	0	8		1	0	0	1
Manufacturing (31-33)	585	20	35	530		270	13	27	230
Mining (21)	498	3	5	490		335	2	3	330
Other Services (81)	194	3	2	189		67	3	0	64
Professional (54)	1,892	793	516	583		630	76	121	433
Public (92)	3,236	22	65	3,149		885	13	30	842
Real Estate (53)	100	5	3	92		44	5	3	36
Retail (44-45)	725	12	27	686		165	10	19	136
Wholesale Trade (42)	80	4	10	66		28	4	7	17
Transportation (48-49)	212	4	17	191		67	3	8	56
Utilities (22)	48	1	2	45		20	1	2	17
Unknown	8,411	5	5	8,401		868	3	3	862
Total	29,207	1,037	819	27,351		5,258	263	307	4,688

Table 4. Number of security incidents and breaches by victim industry and organization size

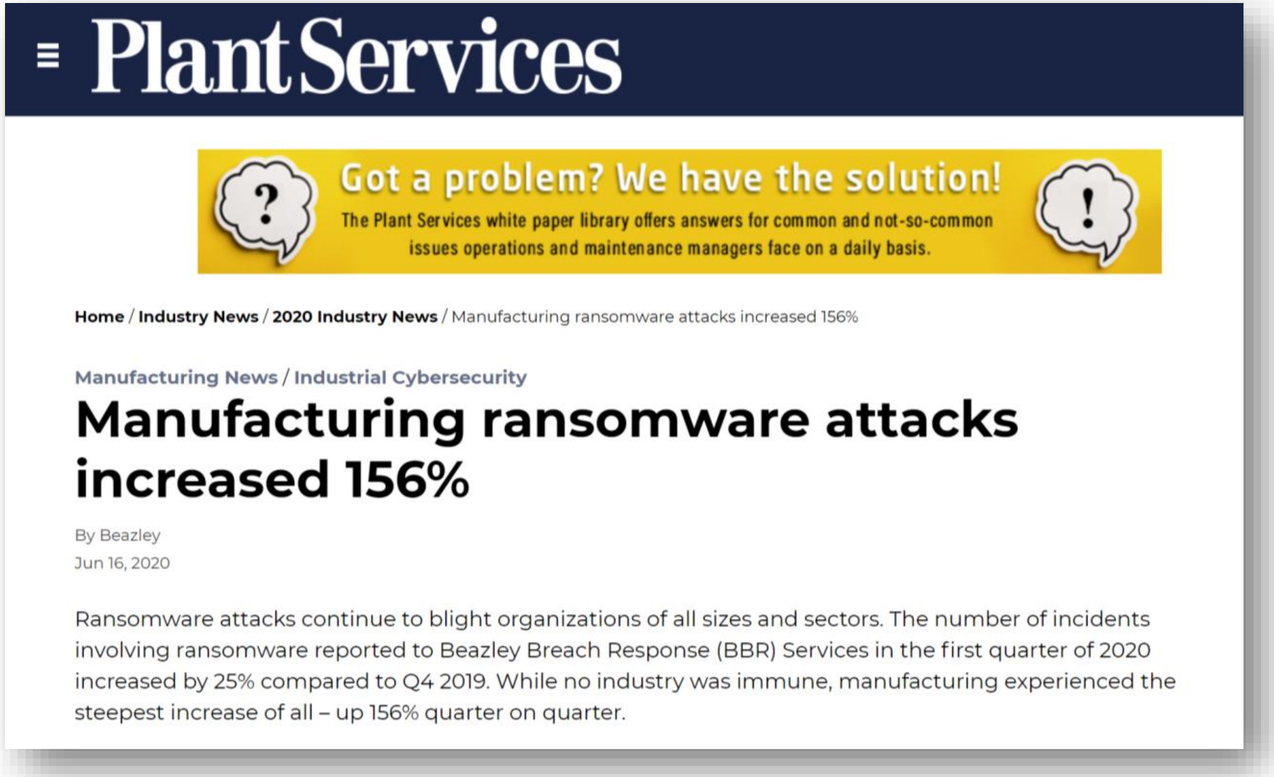
**Verizon 2021 Data Breach Investigations Report*

Manufacturing:



Frequency	585 incidents, 270 with confirmed data disclosure
Top Patterns	System Intrusion, Social Engineering and Basic Web Application Attacks represent 82% of breaches
Threat Actors	External (82%), Internal (19%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Espionage (6%), Convenience (1%), Grudge (1%), Secondary (1%) (breaches)
Data Compromised	Personal (66%), Credentials (42%), Other (36%), Payment (19%) (breaches)

Growing Number of Manufacturing Attacks



Plant Services

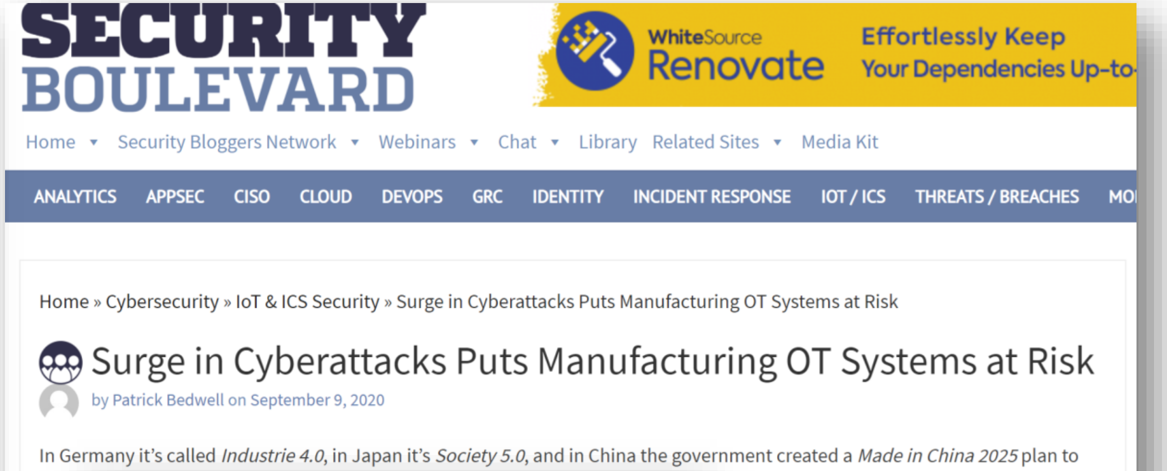
Home / Industry News / 2020 Industry News / Manufacturing ransomware attacks increased 156%

Manufacturing News / Industrial Cybersecurity

Manufacturing ransomware attacks increased 156%

By Beazley
Jun 16, 2020

Ransomware attacks continue to blight organizations of all sizes and sectors. The number of incidents involving ransomware reported to Beazley Breach Response (BBR) Services in the first quarter of 2020 increased by 25% compared to Q4 2019. While no industry was immune, manufacturing experienced the steepest increase of all – up 156% quarter on quarter.



SECURITY BOULEVARD

Home ▾ Security Bloggers Network ▾ Webinars ▾ Chat ▾ Library Related Sites ▾ Media Kit
ANALYTICS APPSEC CISO CLOUD DEVOPS GRC IDENTITY INCIDENT RESPONSE IOT / ICS THREATS / BREACHES MO

Home » Cybersecurity » IoT & ICS Security » Surge in Cyberattacks Puts Manufacturing OT Systems at Risk

Surge in Cyberattacks Puts Manufacturing OT Systems at Risk

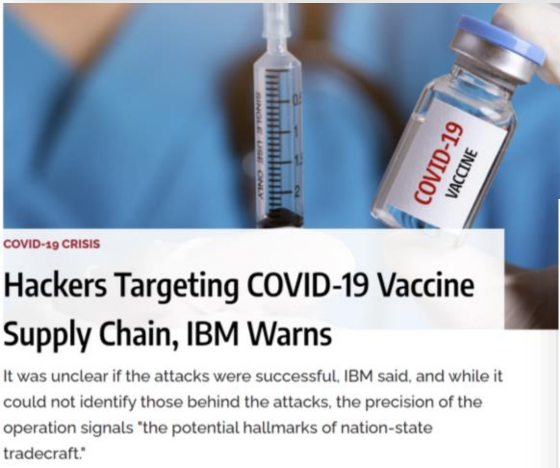
by Patrick Bedwell on September 9, 2020

In Germany it's called *Industrie 4.0*, in Japan it's *Society 5.0*, and in China the government created a *Made in China 2025* plan to dev … Fourth Industrial Revolution.[1] While not identical, eac … ng, and therefore operational technology (OT) sec

It s … s and the free-flowing movement of data? In rea … more important.

Un

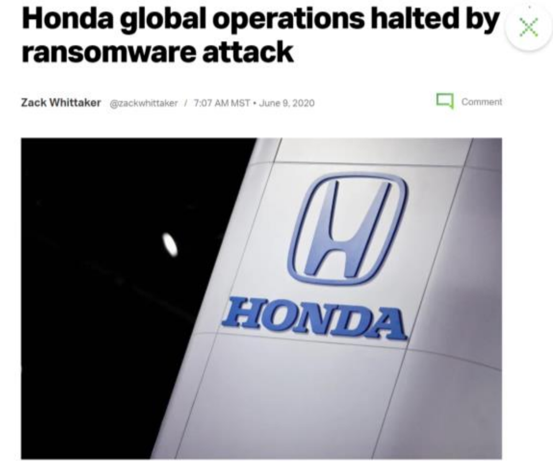
prc



COVID-19 CRISIS

Hackers Targeting COVID-19 Vaccine Supply Chain, IBM Warns

It was unclear if the attacks were successful, IBM said, and while it could not identify those behind the attacks, the precision of the operation signals "the potential hallmarks of nation-state tradecraft."



Honda global operations halted by ransomware attack

Zack Whittaker @zackwhittaker / 7:07 AM MST • June 9, 2020 Comment

- Supply chain attacks are up 78% in 2019. *(Symantec)*
- Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%. *(Varonis)*
- Smaller organizations (1–250 FTEs) have the highest targeted malicious email rate at 1 in 323. *(Symantec)*

https://www.plantservices.com/industrynews/2020/manufacturing-ransomware-attacks-increased-156/
https://techcrunch.com/2020/06/09/honda-ransomware-snake/
https://securityboulevard.com/2020/09/surge-in-cyberattacks-puts-manufacturing-ot-systems-at-risk/
https://www.varonis.com/blog/cybersecurity-statistics/

Financial Impact of Attacks on Manufacturers

Study confirms Manufacturing companies are more vulnerable to Cyber Attacks

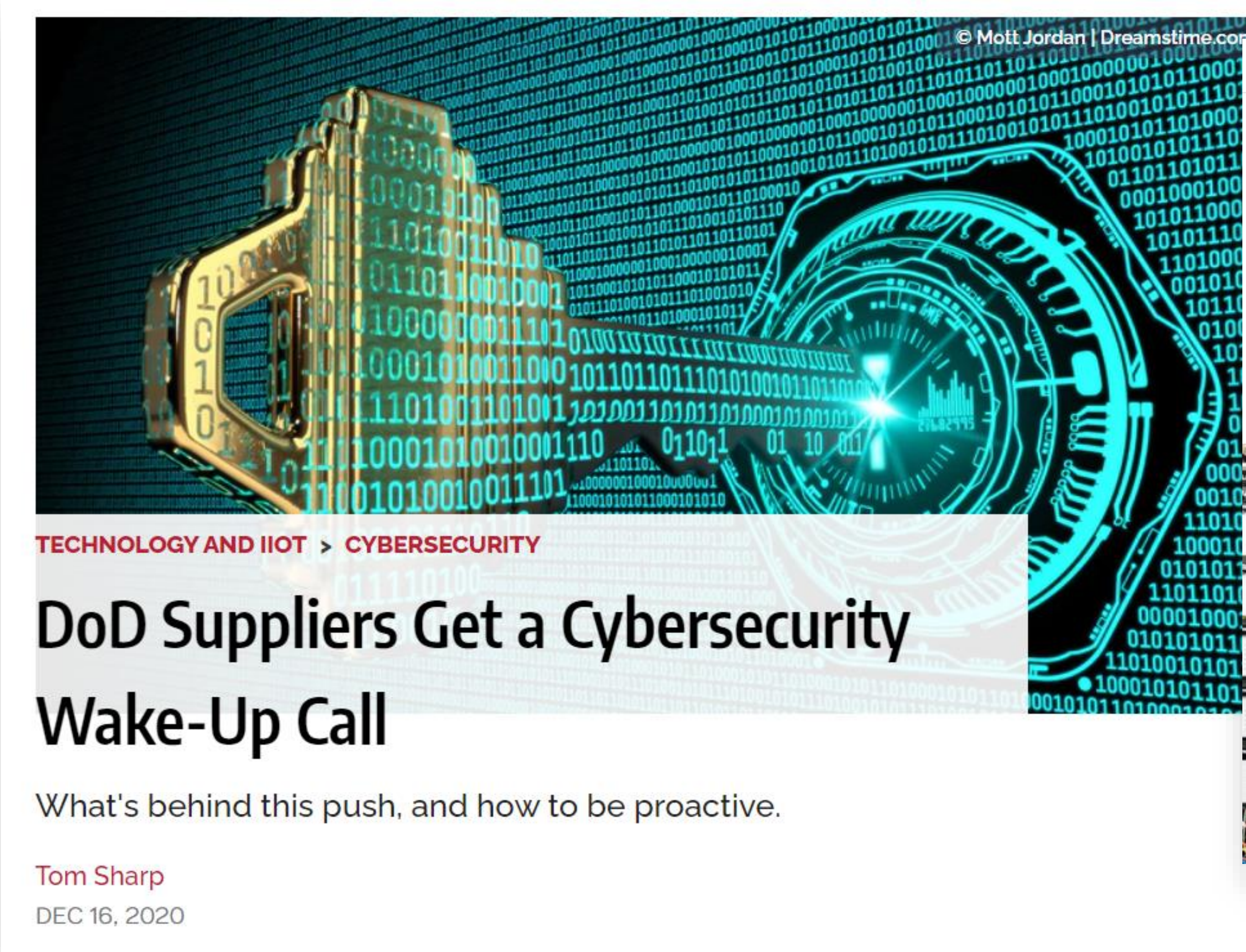
Posted By **Naveen Goud**

https://www.cybersecurity-insiders.com/study-confirms-manufacturing-companies-are-more-vulnerable-to-cyber-attacks/

"According to MAPI, 40 percent of manufacturing firms experienced a cyber attack in the previous year. 38 percent of those firms suffered over $1 million in damages."

Deloitte Manufacturers Alliance for Productivity and Innovation (MAPI) Study

DOD Interim Rule November 30, 2020



© Mott Jordan | Dreamstime.com

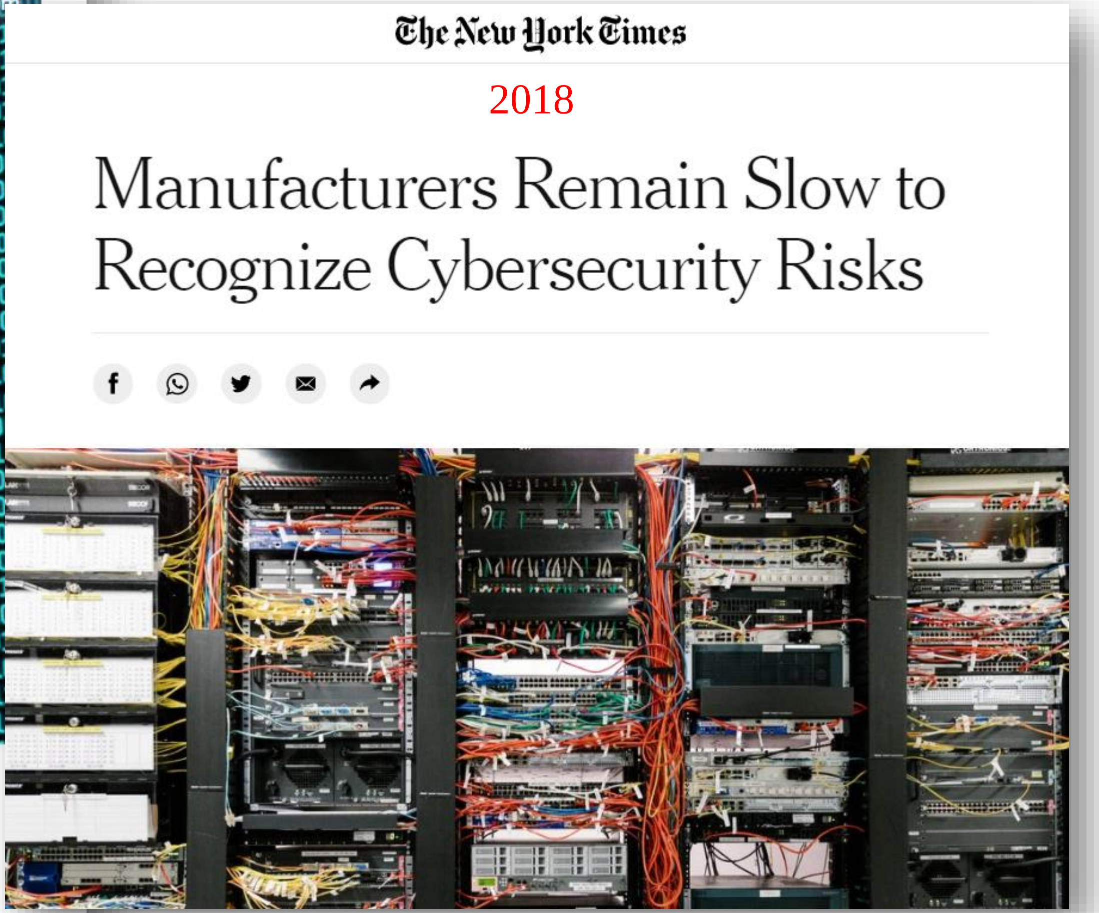
TECHNOLOGY AND IIOT > CYBERSECURITY

DoD Suppliers Get a Cybersecurity Wake-Up Call

What's behind this push, and how to be proactive.

Tom Sharp

DEC 16, 2020



The New York Times

2018

Manufacturers Remain Slow to Recognize Cybersecurity Risks

https://www.industryweek.com/technology-and-iiot/cybersecurity/article/21150595/dod-suppliers-get-a-cybersecurity-wakeup-call

Impact of Compliance Demands & Regulatory Actions on Business

SMBs pay $11,700 per year, per employee on average in regulatory costs.

The costs of regulation on businesses with less than 50 FTEs are nearly 20% higher than larger companies.

The costs of federal regulations on SMBs is estimated to total over $40B annually.

73% of firms believe regulatory changes will increase the personal liability of senior managers.

More than 67% of organizations expect regulatory compliance costs to increase over the next 12 months.

California is the most regulated state, with 395,608 restrictions; Idaho is the least regulated, with 38,961 regulatory restrictions.

https://www.uschamberfoundation.org/smallbizregs/
https://corporate.thomsonreuters.com/Cost-of-Compliance-2020

xceptional.com

> *"Managing regulatory change was reported as the top compliance challenge in 2020. 34% of companies report outsourcing some or all of their compliance, up from 28% in 2019.*
>
> *- Thomson Reuters Cost of Compliance 2020 Report.*

Victory Media Research, Surveys 2020-2021

What is CMMC…And Why Should You Care?

What Is the CMMC?

The **Cybersecurity Maturity Model Certification (CMMC)** is a new cybersecurity framework and accompanying certification by the US Department of Defense (DoD). The goal of the new CMMC compliance requirement is **to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).**

This new umbrella standard includes requirements from NIST 800-171, the Federal Acquisition Requirements (FAR) document 52.204-21, and beyond. There are five levels of CMMC certification. Each level requires more practices and controls than the previous. Most organizations will have to comply with either Level 1 or Level 3. The **certification is valid for three years.**

Starting this year, contracts offered by the DoD might specify a level of the CMMC required to be a
will require a CMMC certification. Unlike for the current NIST 800-171 requirements there will be r
audit will be performed by Certified 3rd Party Assessor Organizations (C3PAO)

Which Level of CMMC Will We Need?

The CMMC level mandated will be stated in the contract information. The majority of contracts wil
As a general rule:

- If your company will receive exclusively FCI under the contract, then your will need CMMC Level 1
- However, if your organization will receive CUI in addition, then CMMC Level 3 will be required as a

When Will This Be Required?

The DoD **started rolling out** CMMC compliance requirements for new contracts **beginning of 2021.**
contract will have a CMMC level requirement in place. Approximately 15 prime contractors and 15
2021.

> **“If you are unable to comply with new mandatory requirements,” says one of the memos, “GE Aviation will be unable to continue to do business with your company.”**
>
> *Regarding the DoD interim rule in November for Documenting Assessment actions around NIST 800-171 as a foundation for CMMC*

Cybersecurity Maturity Model Certification (CMMC) Considerations

- **Compliance is complex and can be costly.**
- **CMMC is DoD Business Focused (at the moment). Could expand.**
- **Different Usage of Plan of Action & Milestones (POAMs).**
- **Can’t leverage 3rd party’s CMMC designation (No Piggybacking).**
- **Estimates from the Government are for the assessment only.**
- **Some CMMC costs can be included within contracts; but many cannot.**
- **This is a journey; there is no “end state”.**

Resources:
https://www.acq.osd.mil/cmmc/draft.html
https://americansecuritytoday.com/cmmc-first-steps-for-any-organization-seeking-certification/

Panel Questions

How Should Organizations Assess their Readiness to Become CMMC Compliant?

What Are the Key Steps for Achieving and Maintaining CMMC Compliance?

What Technology Changes Should Companies Plan for as They Deal with CMMC?

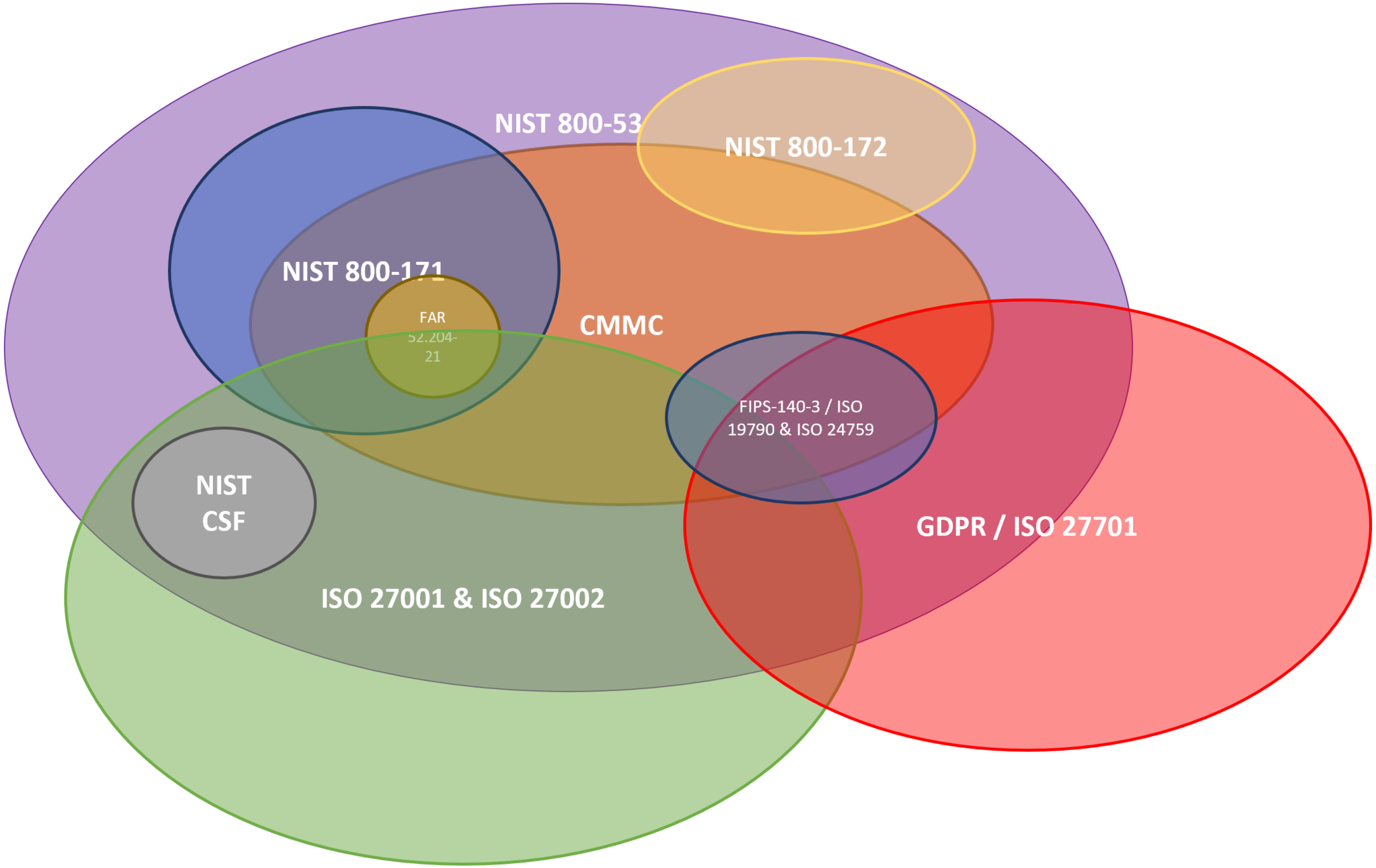
How Much Should Organizations Budget to Address CMMC Compliance?

Note: A report by the Ponemon Institute found that the average cost of compliance for an organization was $5.5 million. Meanwhile, the average cost of noncompliance was over $14.5 million.

GO FORWARD GUIDANCE

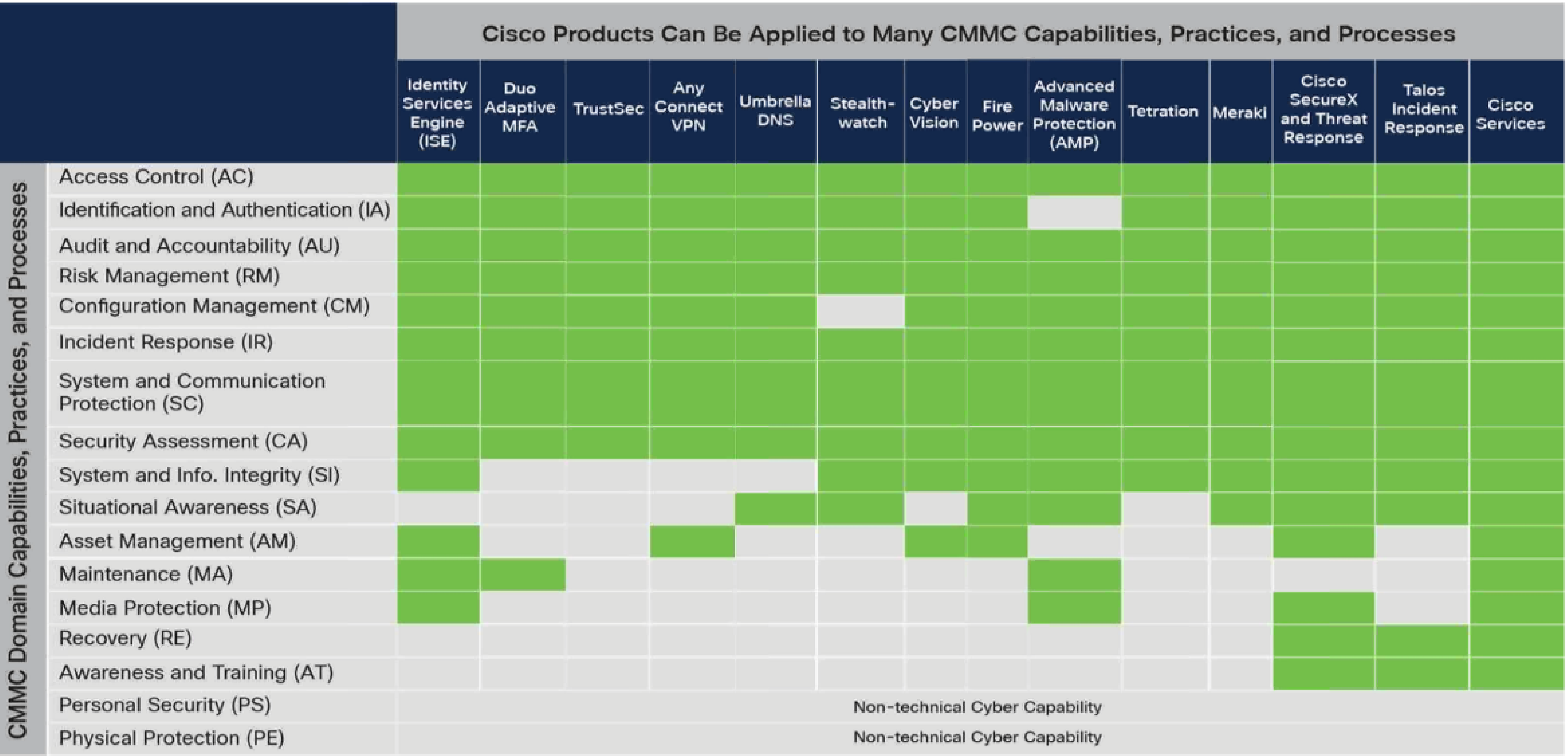
How can manufacturing organizations proactively get ahead of CMMC and other compliance changes while improving how their ability to identify, detect, and respond to cyber threats and attacks?

CMMC as Compared to Other Compliance Frameworks



- Compliance is complex and can be costly.
- Very few companies have the time, resources to manage the process.
- Leverage Xceptional and Cisco to help reduce compliance complexity and improve your CMMC readiness.
- Cisco's Best in Class Technologies Supported by an Award-Winning & Innovative MSP & IT Integration Company.

Cisco = Supporting CMMC



CMMC Domain Capabilities, Practices, and Processes	Cisco Products Can Be Applied to Many CMMC Capabilities, Practices, and Processes													
	Identity Services Engine (ISE)	Duo Adaptive MFA	TrustSec	Any Connect VPN	Umbrella DNS	Stealth-watch	Cyber Vision	Fire Power	Advanced Malware Protection (AMP)	Tetration	Meraki	Cisco SecureX and Threat Response	Talos Incident Response	Cisco Services
Access Control (AC)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Identification and Authentication (IA)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩
Audit and Accountability (AU)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Risk Management (RM)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Configuration Management (CM)	🟩	🟩	🟩	🟩	🟩		🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Incident Response (IR)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
System and Communication Protection (SC)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Security Assessment (CA)	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
System and Info. Integrity (SI)	🟩					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Situational Awareness (SA)					🟩	🟩		🟩	🟩		🟩	🟩	🟩	🟩
Asset Management (AM)	🟩			🟩			🟩	🟩				🟩		🟩
Maintenance (MA)	🟩	🟩							🟩					🟩
Media Protection (MP)	🟩								🟩			🟩		🟩
Recovery (RE)												🟩	🟩	🟩
Awareness and Training (AT)												🟩	🟩	🟩
Personal Security (PS)	Non-technical Cyber Capability													
Physical Protection (PE)	Non-technical Cyber Capability													

Cisco Solutions for NIST Cybersecurity Framework

Identify	Protect	Detect	Respond	Recover
Identity Services Engine	Secure Endpoint	Secure Endpoint	Threat Response	Third party
Secure Network Analytics	Identity Services Engine - RTC	Secure Network Analytics	Identity Services Engine - RTC	
Secure Access by DUO	Secure Firewall	Secure Firewall-Snort	Secure Malware Analytics	
Secure Workload	Secure E-Mail	Umbrella	Talos	
	Cloudlock	Secure Mobility Client	Umbrella-Investigate	
	Secure Access by DUO	Secure Workload		

XceptionalCare, vCISO, Advisory, Security as a Service, Compliance as a Service

Support and Monitoring Services

- 24x7 Monitoring and Alerting
- Managed Detection & Response (SIEM/SOC)
- Unlimited Helpdesk Support 6:00 a.m. – 6:00 p.m. M-F
- End Point Detection & Response with Anti-Virus and Patching
- Password Vault and Document Repository
- IT Asset Management
- Desktop/Email/Server Backups
- Mobile Device Management
- Single Sign On with Multifactor Authentication

Benefits

- Comprehensive Blanket IT Support, Security & CMMC Managed Services
- Predictable Cost Per User/Asset
- Access to Dedicated Engineers

IT Management, Consulting & Compliance Services

- Virtual CIO Strategy and Planning
- Hardware/Software Architecture, Design, Implementation, Resale
- Quarterly Security Assessments
- CMMC Compliance Manager
- Performance Tuning
- End-User Security Training and Phishing Tests

CMMC:

✓ Compliance Manager CMMC One-time Set Up
✓ Annual Subscription
✓ CMMC Compliance Manager Software
✓ Quarterly Scans
✓ Assessment Report Delivery
✓ 1 Hour Report Review/Recommendations Session

Reports & Assets Included:

✓ NIST 800-171 DoD Assessment
✓ Score Report
✓ System Security Plan (SSP)
✓ Plan of Action and Milestones (POA&M)
✓ NIST 800-171 Scoring Supplement Worksheet
✓ CMMC Assessor Checklist
✓ CMMC Risk Treatment Plan
✓ CMMC Risk Analysis
✓ CMMC Evidence of Compliance
✓ Additional Supporting Documents & Worksheets

Cisco Zero Trust Security for CMMC

Addresses level 1-5 domain capacities

CMMC Levels
#1 Basic Cyber Hygiene
#2 Intermediate Cyber Hygiene
#3 Good Cyber Hygiene
#4 Proactive Cyber Hygiene
#5 Advanced Cyber Hygiene

Product	Capability	1	2	3	4	5
ESA/WSA	Advanced threat protection capabilities to detect, block and remediate threats	□	■	■	■	■
Umbrella	Advanced defense and intelligence against threats	■	■	■	■	■
Duo	Establish user trust w/multi-factor auth, SSO for SaaS and device visibility	■	■	■	■	■
Cyber Vision	Threat detection/intelligence for cyber threats in the industrial networks	□	■	■	■	■
AnyConnect	Remote access to network with visibility and posture compliance via agent	■	■	■	■	■
SDA/ISE/TrustSec	Wired, wireless, VPN access policy with network segmentation	■	■	■	■	■
Tetration	Threat detection/intelligence for threats in the private/hybrid clouds	■	■	■	■	■
AMP/Threat Grid	Threat detection/intelligence with host visibility and remediation	□	■	■	■	■
Stealthwatch	Threat detection with internal network and cloud visibility via flow sensors	□	■	■	■	■
Threat Response	Threat visibility and rapid containment with intel-driven incident response	□	■	■	■	■
Firepower	Network access, segmentation and threat detection with in-line insertions	■	■	■	■	■

Key Decisions, Options

Delay & Denial:

The Highest Risk Option

Templates & Tool Kits:

Confusion, Gaps, Corrective Action

Deflect, Defer:

Proof of Compliance is Still on You

Baby Steps:

Find an Advisor, Get Some Advice

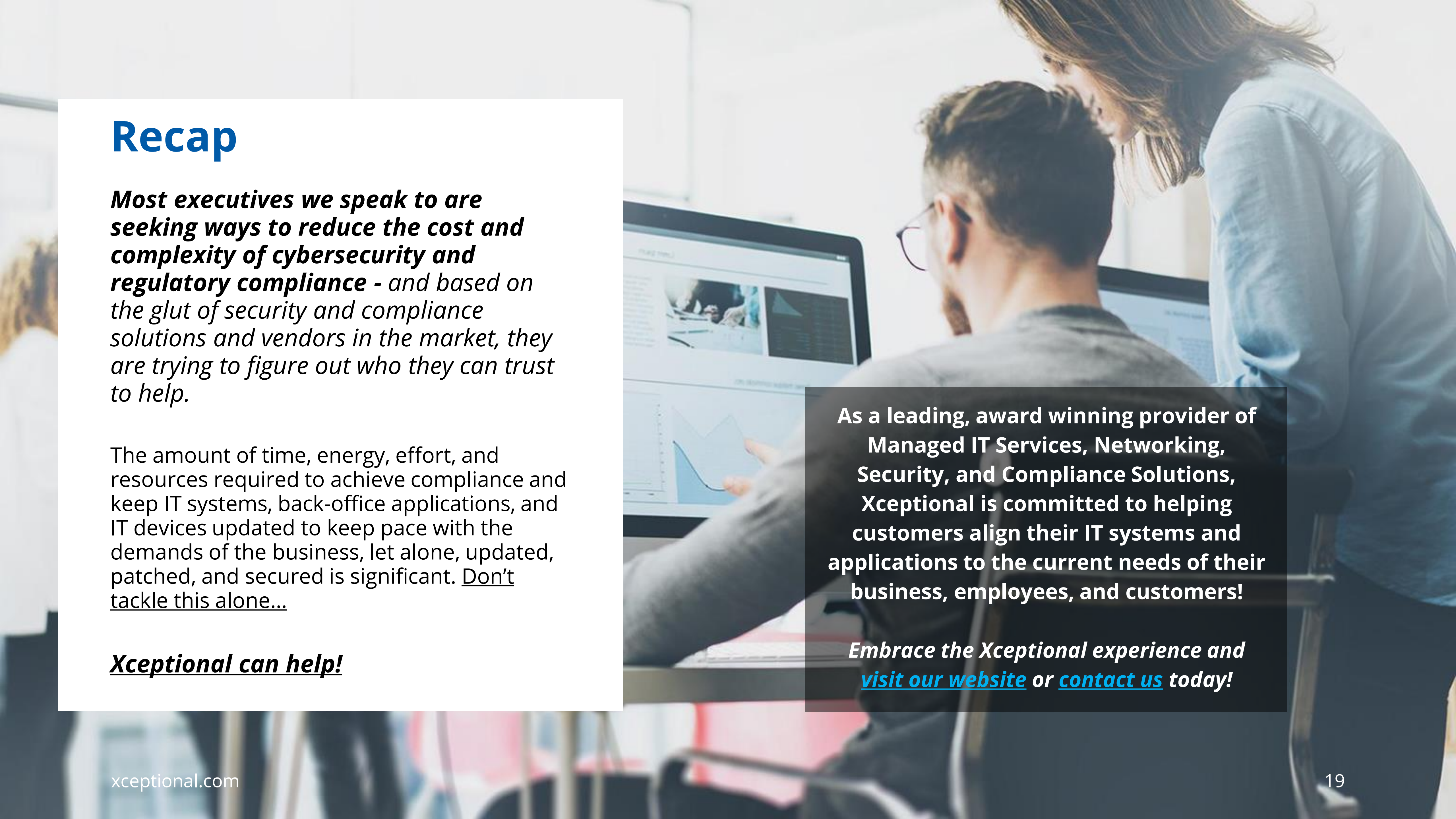
Begin to Act:

Assessments, Gap Analysis, Remediation

Find Cost Effective Solutions:

Find a Partner & Outsource

Victory Media Research, Surveys 2020-2021



Recap

Most executives we speak to are seeking ways to reduce the cost and complexity of cybersecurity and regulatory compliance - *and based on the glut of security and compliance solutions and vendors in the market, they are trying to figure out who they can trust to help.*

The amount of time, energy, effort, and resources required to achieve compliance and keep IT systems, back-office applications, and IT devices updated to keep pace with the demands of the business, let alone, updated, patched, and secured is significant. Don’t tackle this alone…

Xceptional can help!

As a leading, award winning provider of Managed IT Services, Networking, Security, and Compliance Solutions, Xceptional is committed to helping customers align their IT systems and applications to the current needs of their business, employees, and customers!

Embrace the Xceptional experience and visit our website or contact us today!

Drawing!

Registration Gift - First 10 people to register will receive a $25 amazon & Xceptional Swag bag

Attendee Gift - First 20 people will receive a $25 visa card

Bonus Gift

AppleTV ($200)

Bonus Gift

Security Door Bell ($200)

Bonus Gift

Home Security System ($300)

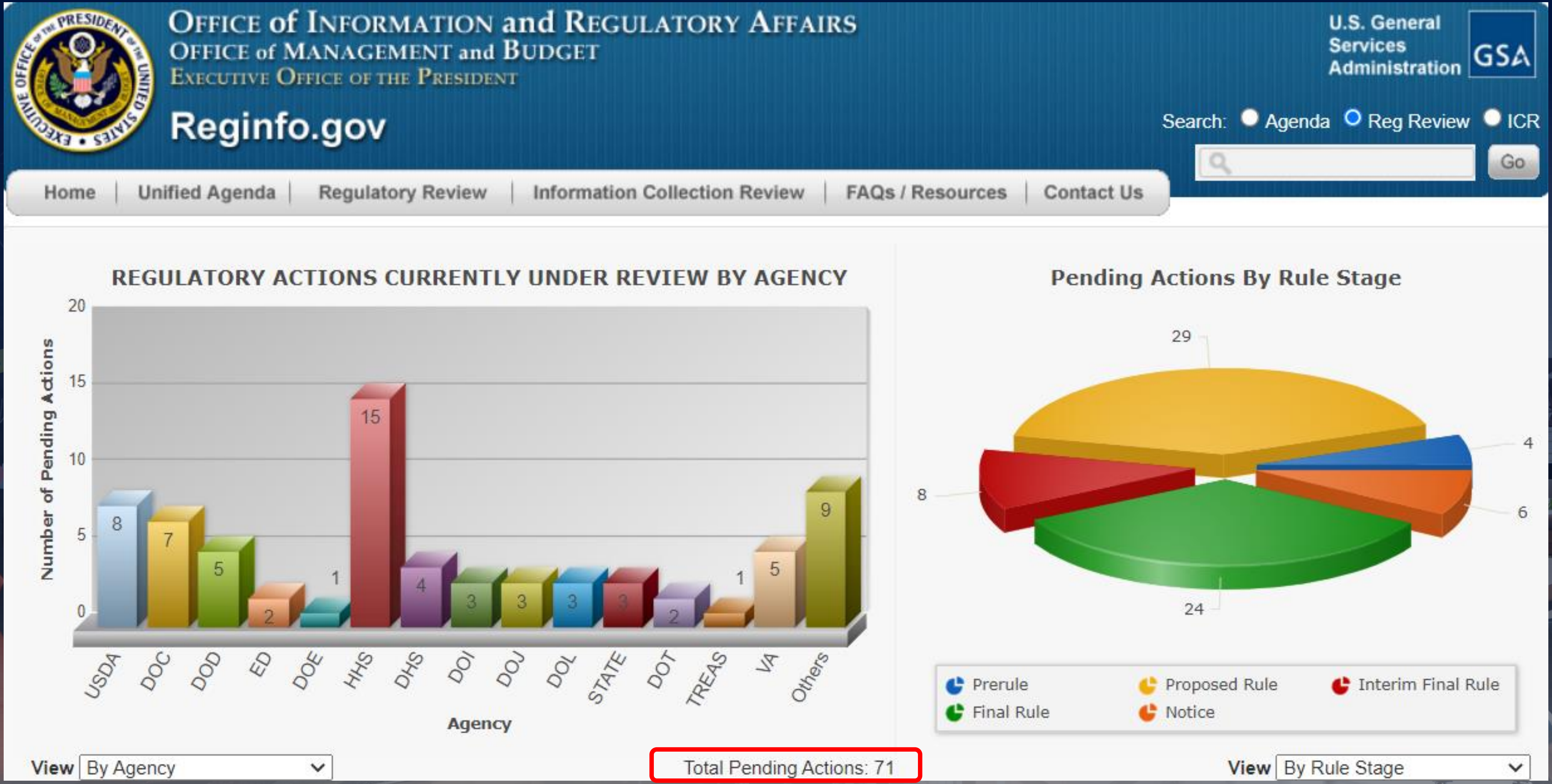
Xceptional | Tech Data | Cisco Partner

Thank You!

Visit our **resources page** to access our free eBooks and research!
Request a **complimentary network** or **security assessment**!

xceptional.com | 858-225-6230

Regulatory Compliance Rate of Change: Reginfo.gov


OFFICE of INFORMATION and REGULATORY AFFAIRS
OFFICE of MANAGEMENT and BUDGET
EXECUTIVE OFFICE OF THE PRESIDENT
Reginfo.gov
U.S. General Services Administration
GSA
Go
Home
Unified Agenda
Regulatory Review
Information Collection Review
FAQs / Resources
Contact Us
REGULATORY ACTIONS CURRENTLY UNDER REVIEW BY AGENCY
Number of Pending Actions
0
5
10
15
20
8
7
5
2
1
15
4
3
3
3
3
2
1
5
9
USDA
DOC
DOD
ED
DOE
HHS
DHS
DOI
DOJ
DOL
STATE
DOT
TREAS
VA
Others
Agency
Pending Actions By Rule Stage
29
4
6
24
8
Prerule
Proposed Rule
Interim Final Rule
Final Rule
Notice

Search: ○ Agenda ● Reg Review ○ ICR

View By Agency

Total Pending Actions: 71

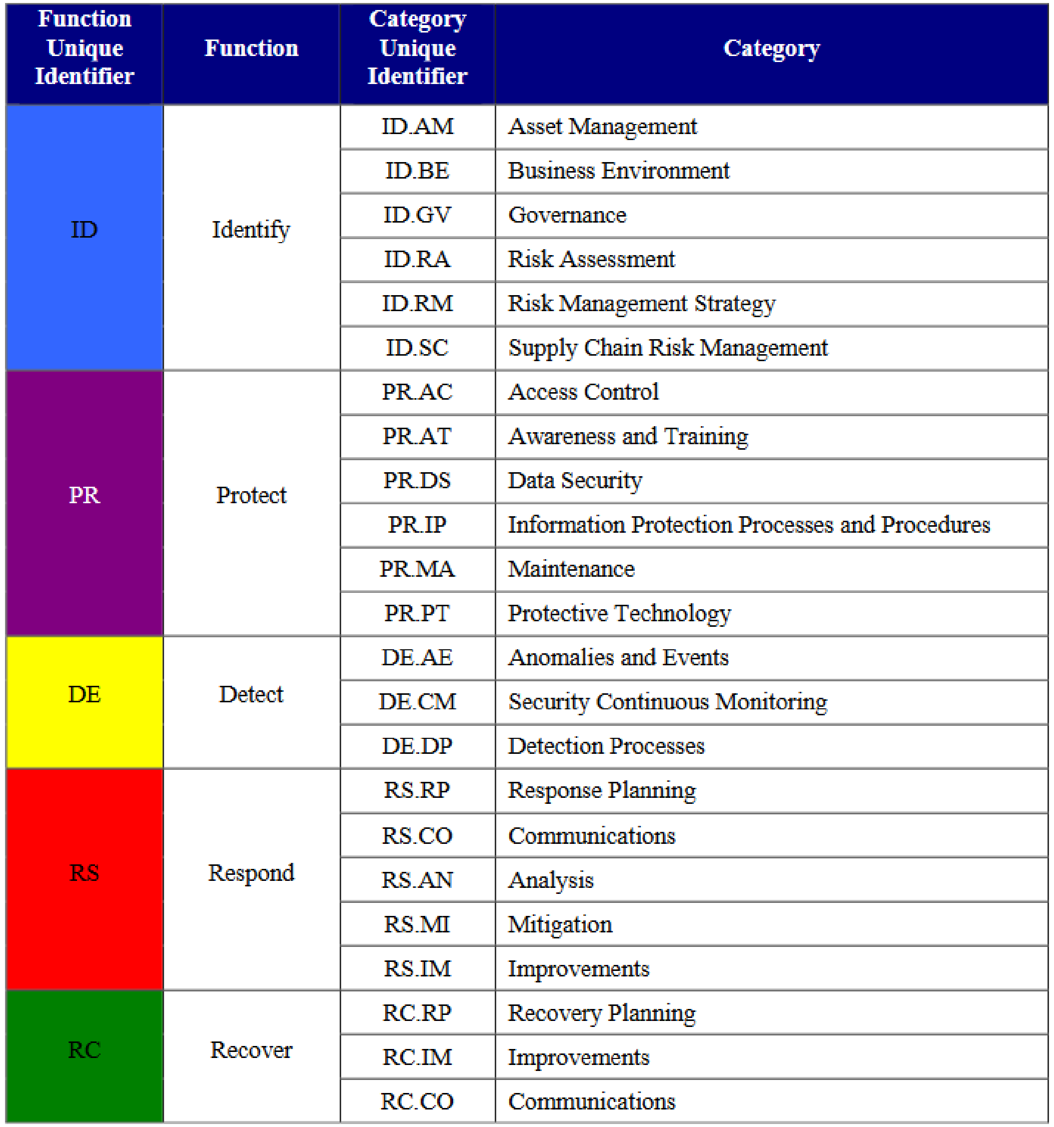
View By Rule Stage

August 26, 2021

NIST

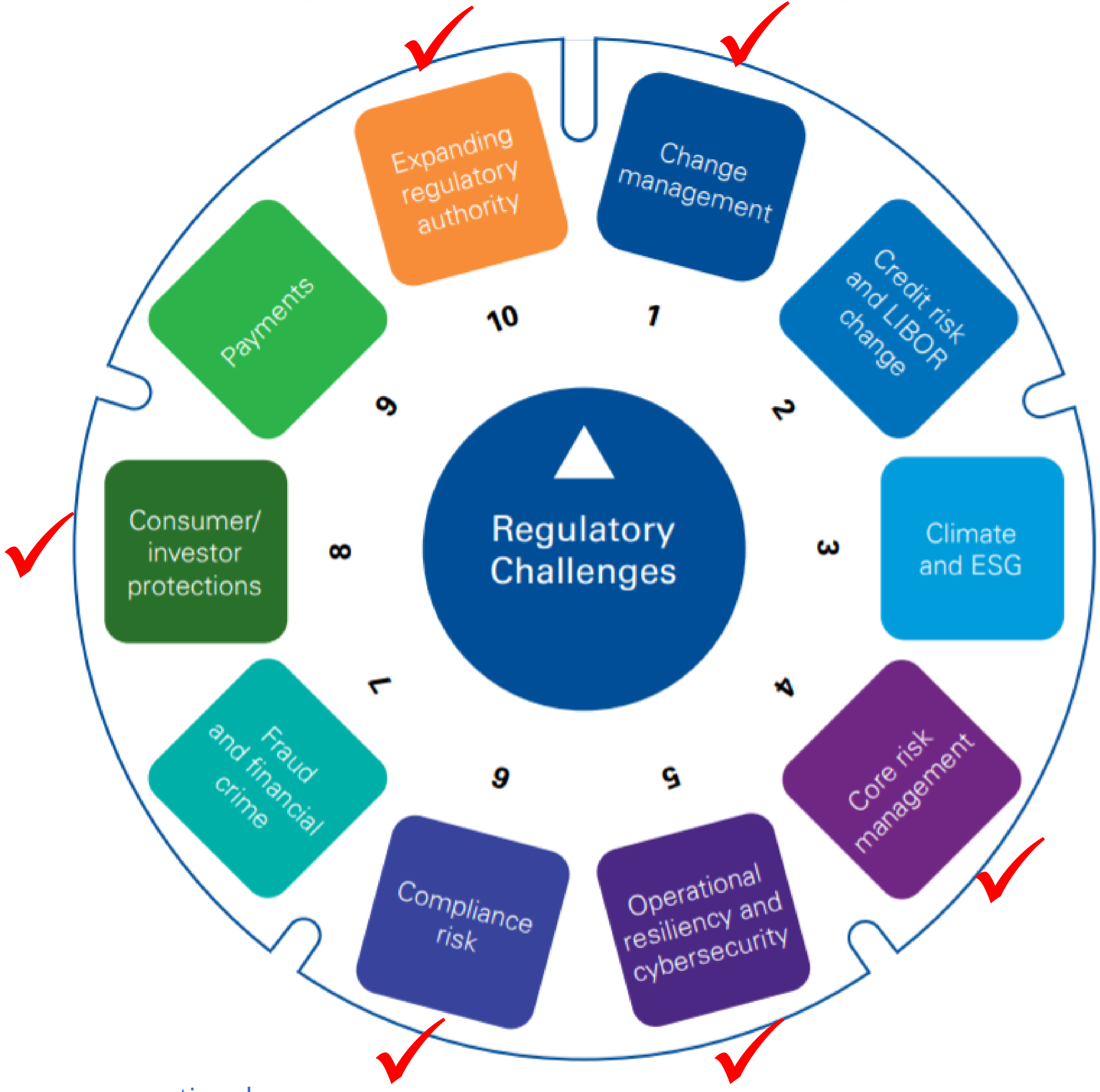
Organizations that operate within or support organizations in regulated industries need a program that (among other things):

- **Inventories and correctly classifies assets** according to risk
- **Periodically scans and assesses** unpatched software and system vulnerabilities
- **Identifies malicious entities probing systems** and network
- **Continuously monitors network traffic and system events** for potential unsecure behaviors
- **Responds to identified malicious events** to remediate them
- **Has the ability to audit and report** effectiveness



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	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

10 Key Regulatory Challenges (KPMG)



Regulatory Challenges

1 Change management ✓

2 Credit risk and LIBOR change

3 Climate and ESG

4 Core risk management ✓

5 Operational resiliency and cybersecurity ✓

6 Compliance risk ✓

7 Fraud and financial crime

8 Consumer/ investor protections ✓

9 Payments

10 Expanding regulatory authority ✓

5 GREATEST COMPLIANCE CHALLENGES

1. Balancing budgets and increasing compliance costs
2. Volume of regulatory change
3. Driving demonstrable culture change
4. Increased personal liability
5. Implementation and embedding of regulatory changes

Thomson Reuters, 2020