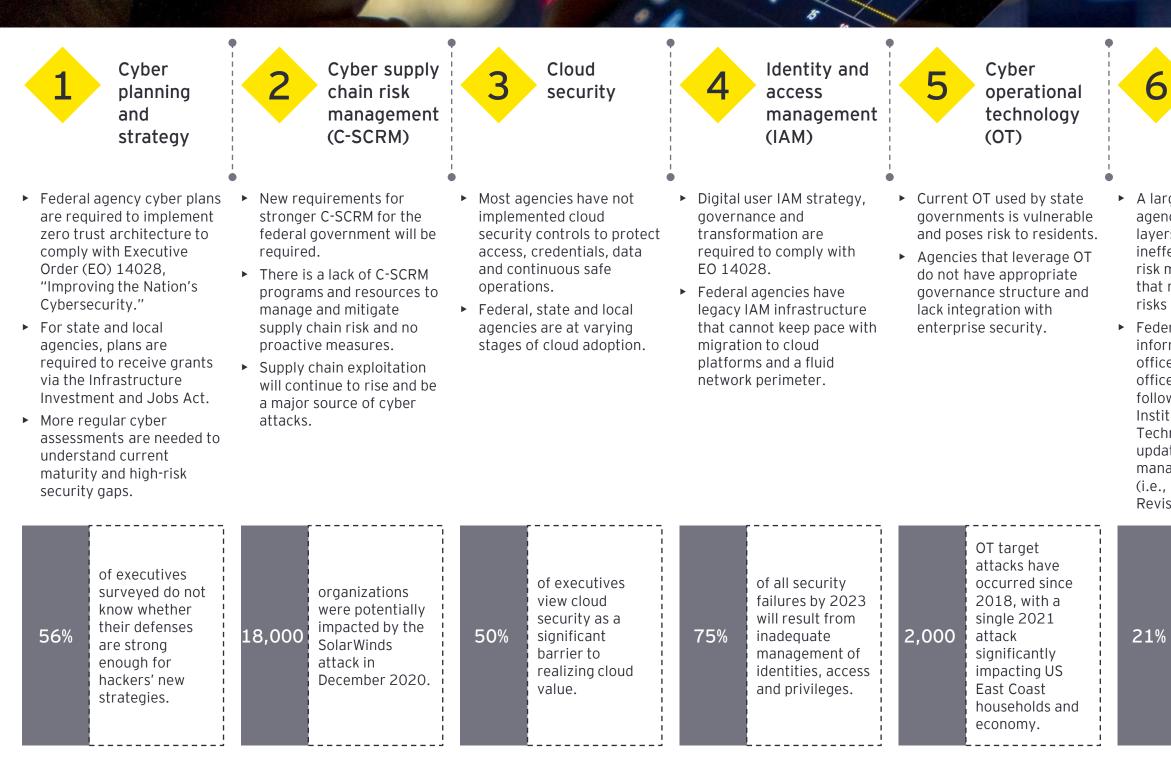


Top government and public sector cyber trends



Risk management framework (RMF)

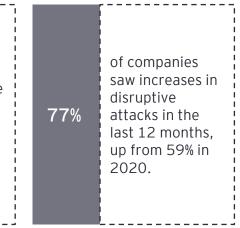
A large number of federal agencies have accumulated layers of redundant, ineffective and misaligned risk management controls that rarely address cyber risks sufficiently.

 Federal agency chief information security officers and chief privacy officers are revisiting RMFs following the National Institute of Standards and Technology (NIST) 2020 update to its flagship risk management guidance (i.e., SP 800-53 Revision 5).

> of organizations currently believe they have an effective framework to mitigate risk.

Ransomware readiness and resilience (R3)

- ► A large number of agencies don't have playbooks to respond to ransomware systematically to limit mission and financial impact.
- Overreliance exists on cyber insurance as the primary means to protect against ransomware.
- Lack of basic cyber hygiene causes most ransomware attacks.



How can Ernst & Young LLP help?

 I Cyber planning and strategy EY cyber program assessment Diagnostic capability tied to NIST security domains Maps to multiple compliance standards and security frameworks Benchmarking across multiple capability areas Results in actionable road map with initial cost estimates, project priority and implementation level of effort to include "quick win" opportunities 	 2 2 3 4 4<	 Cloud security focus areas Cloud security focus areas Cloud security assessment framework Cloud security posture management - tracks and protects against misconfigurations Micro-segmentation and zero trust - limit the risk of lateral movement and insider threats Hardware security module - device designed to store secret keys used to verify certificates and encrypt and decrypt data 	 4 Identity and access management (IAM) The EY Cybersecurity IAM offering includes the following: IAM architecture and engineering Unique integration capabilities between IAM systems to provide complete governance across the IAM stack (e.g., privileged access management and identity governance systems integration) Zero trust architecture for IAM Ability to stand up a program within weeks with skilled resources hard to find in industry 	 5 Gyber operational technology (OT) EY OT cybersecurity offering includes the following enablers: OT cybersecurity governance Roles and responsibilities Use of artificial intelligence/machine learning and risk analytics to provide an evidence- based business risk and cyber risk exposure Supports mapping to NIST security controls 	 Anterior of the second state of the s	 7 Ransomware geadiness and readiness and resilience (R3) The EY R3 solution has: Understanding of unique risks and enumeration for rapid remediation Enhanced capability to identify, protect, detect, respond and recover from a ransomware event Action to secure business operations
Client examples						
 Cyber program and maturity assessments for multiple state agencies Development of cyber strategy and road maps for state agencies 	 Governance, risk and compliance technology implementation and process design for third- party risk management processes Ongoing support for a transportation authority 	 Cloud strategy development, implementation and migration, including security controls and processes Cloud application modernization and cloud data governance and controls for a US military service 	 User identity governance architecture for a large federal agency component that reduced IT audit findings from 41 down to 1 in two years IAM stacks for three components of a Global 360 account 	 Setup of an OT security operation center for a state department of transportation Security assessment of OT capability for transportation authority 	Multiple RMF strategy and engineering engagements for a US military service and five federal agencies	 Ransomware readiness assessment for a state agency Response to multiple malware and ransomware incidents Tabletop exercise for state health agencies

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP. All Rights Reserved.

2202-3985647 ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com