EY

Building a better working world

Top government and public sector cyber trends

1 Cyber planning and strategy

- Federal agency cyber plans are required to implement zero trust architecture to comply with Executive Order (EO) 14028, "Improving the Nation's Cybersecurity."
- For state and local agencies, plans are required to receive grants via the Infrastructure Investment and Jobs Act.
- More regular cyber assessments are needed to understand current maturity and high-risk security gaps.

56% of executives surveyed do not know whether their defenses are strong enough for hackers' new strategies.

2 Cyber supply chain risk management (C-SCRM)

- New requirements for stronger C-SCRM for the federal government will be required.
- There is a lack of C-SCRM programs and resources to manage and mitigate supply chain risk and no proactive measures.
- Supply chain exploitation will continue to rise and be a major source of cyber attacks.

18,000 organizations were potentially impacted by the SolarWinds attack in December 2020.

3 Cloud security

- Most agencies have not implemented cloud security controls to protect access, credentials, data and continuous safe operations.
- Federal, state and local agencies are at varying stages of cloud adoption.

50% of executives view cloud security as a significant barrier to realizing cloud value.

4 Identity and access management (IAM)

- Digital user IAM strategy, governance and transformation are required to comply with EO 14028.
- Federal agencies have legacy IAM infrastructure that cannot keep pace with migration to cloud platforms and a fluid network perimeter.

75% of all security failures by 2023 will result from inadequate management of identities, access and privileges.

5 Cyber operational technology (OT)

- Current OT used by state governments is vulnerable and poses risk to residents.
- Agencies that leverage OT do not have appropriate governance structure and lack integration with enterprise security.

2,000 OT target attacks have occurred since 2018, with a single 2021 attack significantly impacting US East Coast households and economy.

6 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).

21% of organizations currently believe they have an effective framework to mitigate risk.

7 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.

77% of companies saw increases in disruptive attacks in the last 12 months, up from 59% in 2020.

Sources: EY Global Information Security Survey (GISS) 2021, Govtech, PWC

How can Ernst & Young LLP help?

1 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 Cyber supply chain risk management (C-SCRM)

EY C-SCRM offering

- Proprietary risk-scoring capability that utilizes commercial data sets resulting in custom watch lists
- Combination of multiple data streams to include financial, geopolitical and technical factors
- Alignment to NIST compliance standards
- Ongoing monitoring capability to capture new risks over time
- Ability to stand up a program within weeks

3 Cloud security

EY cloud security focus areas

- Cloud security assessment and strategy – align to NIST 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 Cyber 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

6 Risk management framework (RMF)

The EY RMF solution has:

- Next-generation RMF, including assessment, road map and federal strategy (e.g., pre-audit support and alignment with NIST and FedRAMP requirements)
- RMF engineering using governance, risk, and compliance technologies and analytics, as well as robotic process automation
- Authorization to operate acceleration, including risk dashboards

7 Ransomware 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.

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