4 FOCUS AREAS FOR PUBLIC SECTOR TO MITIGATE CYBER-ATTACK RISK
Connecting Security, Risk and Mission Teams to Mitigate Risks from Cyber Attack

Federal, defense and intelligence agencies and state and local governments are innovating and advancing digital transformations to better serve their constituents, protect the homeland, connect and engage citizens, and increase agency efficiency of their missions. These modernizations take advantage of the robust technologies that are empowering communities and individuals to thrive in an evolving, digitally connected world.

While implementing these transformative technologies to drive their missions, government organizations also continue to invest in security technologies to help them protect citizen and government data, infrastructure and systems. However, the evolving threat landscape combined with the rate of change and scope and scale of digital environments is causing many organizations to struggle to keep up with growing cyber-attack risk. The reality is, we live in a world where prevention of cyber attacks remains difficult. Therefore, to mitigate mission risk, organizations need to ensure they are prepared to detect and respond to an attack appropriately across the mission, from SOC to Leadership.

This eBook will help outline four focus areas to mitigate cyber-attack risk to reduce the overall mission impact of a cybersecurity event.
Your agency security team is the front line in detecting cyber attacks and implementing technical responses to contain and remediate threats. All are very important to protecting your organization and their assets; however, in many cases this is where the response stops. While an incident may show up in an executive brief, additional members of the organization should understand pertinent facts and have visibility into:

- What occurred
- Who and what were potentially impacted
- What was done to stop it
- How are we preventing it from happening again

In light of increased legislative and policy pressure, government organizations must be prepared to be more transparent regarding attacks and the steps they take to mitigate future events. Cross-functional teams now have greater responsibility and shorter time frames. For example, federal agencies must report information security incidents, where the confidentiality, integrity or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to the NCCIC/US-CERT with the required data elements, as well as any other available information, within one hour of being identified.

This new dynamic requires that security, risk and mission teams are well-planned and coordinated to effectively respond to an incident from both the technical side, to stop it, and the mission side, to manage the fallout from constituents, partners and other elements of the government.
In order to maximize the investment in cybersecurity tools and technologies, organizations must approach defense of the network and its applications and associated data with a structured process. Employing a digital risk management approach as well as a thoughtful incident management plan will help mitigate impacts. Following these four focus areas and action plans derived from the NIST Cybersecurity Framework can help organizations prepare to detect an incident and manage a coordinated response from security, IT, risk and mission stakeholders.

**STEP 1:** IDENTIFY—BREACH PREPAREDNESS

**STEP 2:** PROTECT & DETECT—RISK REDUCTION & INCIDENT RESPONSE

**STEP 3:** RESPOND—BREACH REMEDIATION

**STEP 4:** RECOVER—POST BREACH ADAPTATION
FOCUS AREA 1: IDENTIFY—INCIDENT PREPAREDNESS

Prepare for an attack before it happens. Develop policies as well as procedures based on established risk tolerance, document workflows to centrally manage investigations and remediation, as well as coordinate a mission response. This provides a repeatable process to triage the incident cross-functionally with coordinated, well-defined plans that reduce effort and complexity.

**PLAN FOR ATTACKS:**

1. **Create workflows to manage investigations** and assure indicators of compromise (IOCs) are correlated across the enterprise. Measure detection and response times to ensure that there is a benchmark for the SOC team.

2. **Establish a central organizational and IT asset catalog** and taxonomy so teams involved are all on the same page.

3. **Document mission response processes** such as compliance reporting, public relations, legal, and internal and external communications so everyone knows their roles and responsibilities.

4. **Test and retest.** Practice mock incidents to make sure the workflows are streamlined and effective to orchestrate the response across the organization.
Focus Area 2: Protect & Detect—Risk Reduction & Incident Response

Departments and agencies are investing and continue to invest in protection technology, processes and people to protect the government’s data, infrastructure and systems. Maximizing the current capabilities is key to connecting the dots across a variety of tools to detect and respond to threats. SOC analysts must be able to cut through the clutter of alerts and empower the security team to detect known and unknown cyber threats with a security platform that provides visibility across all environments. Assist analysts’ forensic investigations by combining insights across various security, IT and mission insights so they can determine the full scope of the attack and formulate actions in a timely manner.

Key Capabilities to Identify Threats:

- **Visibility**
  Across logs, packets, network, endpoint, hosts, Netflow

- **Deep Advanced Analytics**
  Including user and entity behavior analytics (UEBA)

- **Mission Context**
  Including contextual intelligence and asset criticality, DRM asset connection

- **Incident Management**
  Including orchestration and automation

- **Actionable Insights**
  Access and entitlement intelligence, threat intelligence, known vulnerabilities, network infrastructure configuration management
Security teams typically focus on identifying the scope and severity of an incident, but many times they lack the ability to quickly assess the mission impact of the attack. Having performed organizational mission analysis of the network and identifying these mission-critical assets connects security teams with mission and risk context; therefore, organizations can prioritize and orchestrate the right level of response and escalation based on the potential mission impact in downtime, customer confidence, compliance posture, bottom-line financials and more.

INCIDENT REMEDIATION STARTS WITH ASSESSMENT:

- **Provide incident responders context** to Agency asset criticality information to understand mission impact and prioritize appropriately.
- **Integrate Mission Impact Analysis** into investigations to understand the upstream and downstream implications.
- **Conduct cyber-risk quantification** assessments to understand the dollar and mission impact of cyber attacks on critical assets.
- **Incorporate known vulnerability data** into investigations to quickly understand which assets are more vulnerable to help analysts prioritize remediation efforts.
Centralize incident management across functional silos both inside and outside the "glass walls" of the SOC to ensure consistent, coordinated and automated responses. This centralization enables stakeholders a singular view of “what the risk is,” “how bad it is,” “what is impacted” and “what’s being done to address it,” allowing department leadership to make better mission decisions to minimize the impact.

<table>
<thead>
<tr>
<th>INCIDENT: Rapid, Organized Response</th>
<th>TECHNICAL RESPONSE</th>
<th>MISSION RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect and declare incident</td>
<td>Incident declared, automatically invokes organizational response workflows</td>
<td></td>
</tr>
<tr>
<td>Identify the impacted areas</td>
<td>Ensure mission processes are resilient</td>
<td></td>
</tr>
<tr>
<td>Clear, process-oriented escalations</td>
<td>Engage cross-functional teams based on established workflows</td>
<td></td>
</tr>
<tr>
<td>Automation and orchestration to reduce dwell time and contain the threat</td>
<td>• Compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Legal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Communications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• PR/IR</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>POST-incident: Address Vulnerability Gaps</th>
<th>TECHNICAL RESPONSE</th>
<th>MISSION RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forensic analysis</td>
<td>Understand need for new controls or change in processes (root cause for systemic issues)</td>
<td></td>
</tr>
<tr>
<td>Locate assets, applications and protocols leveraged for data exfiltration</td>
<td>Communicate priority and direction to ensure most valuable assets are protected</td>
<td></td>
</tr>
<tr>
<td>Make security changes</td>
<td>Closed-loop process to ensure change management</td>
<td></td>
</tr>
</tbody>
</table>
RSA HELPS YOU MITIGATE CYBER-ATTACK RISK

RSA has the solution to support holistic detection and cross-functional response coordination that connects security, risk and mission stakeholders to mitigate and measure the mission impact from a cyber attack. Aligned with the NIST Cybersecurity Framework, our technology and advisory services help you assess maturity to the framework and implement the tools to help improve that maturity in your agency or department. Our approach is risk-based and focused on helping organizations assess the risk, detect and respond to threats, and ensure controls and processes are enacted to prevent a future occurrence.

HOW WE HELP

RSA CYBER INCIDENT RISK FRAMEWORK
- Engagement
- Assessment
- Benchmark Report
- Cyber Practice Program

EVOLVED SIEM/ADVANCED THREAT DETECTION & RESPONSE
- Security Platform
- Logs & Packets
- Endpoint
- UEBA
- Orchestration & Automation
- Declare Incident Automation with RSA Archer Suite*

INTEGRATED RISK MANAGEMENT
- Cyber Incident & Breach Response
- Vulnerability Program Management
- Business Impact Analysis
- Dashboards & Reporting
- Cyber Risk Quantification
- Extend Business Context to Security Analyst via Context Hub in RSA NetWitness Platform*

SECURE, RISK-BASED ACCESS & AUTHENTICATION
- Risk-Based Authentication
- Authentication Anomaly Detection
- Identity, Governance & Lifecycle Management
- Access Policy Violation Detection
- Threat Aware Authentication - interoperability with RSA NetWitness Platform*

OMNI-CHANNEL FRAUD PREVENTION
- Omni-Channel Fraud Detection
- Advanced Adaptive Authentication
- Real Time Risk Assessment
- Fraud Intelligence

*R Interoperability between products

Are you prepared to mitigate the business risks from cyber attacks? Take our online assessment to see how you stack up: riskassessment.rsa.com
DIGITAL RISK IS EVERYONE’S BUSINESS
HELPING YOU MANAGE IT IS OURS

RSA offers business-driven security solutions that provide organizations with a unified approach to managing digital risk that hinges on integrated visibility, automated insights and coordinated actions. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user access control; and reduce business risk, fraud and cybercrime. RSA protects millions of users around the world and helps more than 90 percent of the Fortune 500 companies thrive and continuously adapt to transformational change.

Find out how to thrive in a dynamic, high-risk digital world at rsa.com.