BeyondTrust

4 Tips for a Robust Cybersecurity Strategy

There is no easy way to deal with cybersecurity risk. Attacks, often driven by nation states, have become more complex and creative, and government agencies frequently lack the resources to respond effectively. Some high-priority targets, such as power utilities, have unique risk profiles that add further challenges.

"At the end of the day, you want to be hitting the things that are most important to your organization and what your biggest risks are," said Bryce Carter, the Chief Information Security Officer for the City of Arlington, Texas, during a recent GovLoop virtual event titled "Elements for a Robust Security Strategy."

Agencies need to gauge the threat landscape carefully, said fellow speaker Jared Edgar, Idaho's Chief Information Security Officer, but frequently they are over-confident in their assessments. "Oftentimes, too many of the risks are unknown in [an] environment," he explained. "And so we have people making assumptions that things are just fine and they're protected, but nobody's really validating that."

Carter and Edgar offered tips on developing a cybersecurity strategy that's tailored to organizational vulnerabilities. Kevin E. Greene, Chief Security Strategist for Public Sector at BeyondTrust, then dug into a specific type of cybersecurity tool — an updated approach to privileged access management (PAM) — that helps agencies protect their end-user identities.

1 START WITH CULTURE

Build a cybersecurity mindset — an agencywide commitment to security practices and protocols — and then work on the technical details. Security should be considered upfront, so elevate your security team, or IT team if that is all you have, to the level of a strategic partner involved in organizational decision-making. Leaders often come in with a great technical game but fail to align it with organizational goals. That needs to change.

2 BE SELECTIVE WITH CYBER TOOLS

There are lots of "silver bullet" solutions and plenty of vendors promoting them. But unless an agency carefully evaluates security options against the agency's particular needs, officials are just throwing darts at a cyber dartboard and could over-rely on ill-suited technology. And what about employee skills? What cyber tools can your workforce use today, what will employees need to learn, and can your agency invest in that training?

"Work with the realities you have. Don't try to solve it's probably headed in the right direction.
all the world's problems. Just focus on the problems you have, the threats you have, and the capabilities you have to [respond]." — Jared Edgar, State of Idaho

3 EMBRACE AI OPPORTUNITIES

Artificial intelligence (AI) is inevitable, so each agency needs a framework to deal with AI-related risk. But AI can be a huge asset in identifying true threats to a network perimeter, among other security uses. For example, out of potentially millions of risks, AI can filter out the perhaps 10 or 15 actual concerns. An effective cybersecurity strategy is like wearing multiple layers on a cold winter day, and AI can be one layer of cyber protection.

4 PRACTICE GOOD GOVERNANCE

At the end of the day, effective security requires effective governance, a framework aligned with the agency's culture and business mission. Within that governance structure, officials need to address protection, detection and response. That is, how is the agency preventing bad things from affecting its systems, data and people? How does it know when something goes wrong? And when something bad does happen, what can the agency do about it? If an agency can answer those questions well, it's probably headed in the right direction.

Protecting Identities: The Need for Privileged Access Management

In the landscape of cybersecurity risk, identity security stands out. Ninety percent of agencies have suffered an identity-related breach, due largely to the fact that agencies don't understand their privilege pathways, or ways threat actors can exploit their identity attack surface. Traditional cybersecurity detection tools are unable to illuminate those paths most likely targeted by threat actors.

An identity-centric approach helps agencies secure the paths to privilege that threat actors try to exploit. It allows agencies to remedy misconfigurations in their identity infrastructure, protect exposed passwords, remove excessive privileges and other problems that leave their identity resources vulnerable. And a modern privileged access management (PAM) solution provides holistic visibility into an agency's identity hygiene and blind spots, simplifies governance and provides intelligent protection to be resilient against identity-related attacks.

In this video interview, Kevin E. Greene, Chief Security Strategist for Public Sector at BeyondTrust, discusses how privileged access security can keep malicious actors at bay.

Topics include:

→ The components of modern identity-focused security
→ How to implement effective privileged access management
→ The need for a holistic approach to identity protection

"More and more organizations [are] moving to cloud and using software as a service [SaaS], which means more privileges and entitlements that expand and expose the identity attack surface. Organizations need a modern PAM solution to help identify, shrink and manage the expansion of the identity attack surface. The goal is to leave no privileges behind."

— Kevin E. Greene, BeyondTrust