Identity and Access Management Educational Aid Talking Points

Purpose: This educational aid is intended to be used to get the conversation started with your board of directors or overseers to make the case of the importance of identity and access management (IAM) and explain the risks associated with not adopting a robust IAM program. This educational aid is not intended to solve all IAM problems but rather to quickly explain the importance of IAM to executives who do not have many cycles to spend on this topic.

The role of cybersecurity within organizations has dramatically changed over the last decade. What was once a responsibility of the IT department has become a foundation of a business that interconnects multiple local data centers, remote cloud applications, supply chain, remote customers, and all connections between them. At the same time, attackers are becoming more sophisticated and threats more severe.

- An alarming 84% of organizations surveyed by Identity Defined Security Alliance experienced identity related breaches in the past year. according to their 2022 Trends in Securing Digital Identities report.
- Cyber incidents are on the rise, costing billions of dollars and compromising critical and sensitive data and resources.
- In today's world, all online systems are targets. Nation states target critical infrastructure or other critical information systems to conduct espionage activities, steal intellectual property, or prepare for later destructive cyberattacks while criminal organizations conduct wide-ranging campaigns seeking to compromise systems to profit by stealing data or simply ransoming system access.

Cybersecurity incidents are costing organizations billions of dollars by compromising data and systems, resulting in privacy breaches and loss of critical data.

- In 2021, Colonial Pipeline, a major Southeast oil pipeline system suffered a major ransomware attack resulting in disruption to the oil/gas distribution system causing long lines at the gas station and panic by consumers. When people think of the Colonial Pipeline attack, they often think of the attackers exploiting the company for money but they don't often realize the root of how the attack happened was a result of a leaked password, an inactive VPN account, and a lack of multifactor authentication – all of which can be summed up as poor identity and access management.

What are the risks associated with not adopting a robust IAM program? There is significant risk in having a poor identity and access management program. Those risks include:

- Potential fines being levied;
- The financial cost of having to pay ransom with no guarantees that you won't suffer a ransomware attack again;
- The financial cost of remediation;
- Reputational damage;
- Uncertainty if cybers insurance will cover the loss.

In the case of Colonial Pipeline they had to pay $5 million in ransom in order to regain control of its system. On top of that they suffered detrimental damage to their brand as fear of a gas shortage caused panic-buying and long lines at gas stations in many states leading to real shortages in certain areas. Additional cyber insurance coverage may not necessarily cover attacks especially if companies fail to establish basic hygiene controls.

What is IAM and how does it help?

- IAM is a framework of business processes, policies, and technologies that facilitate the management of digital identities. It ensures that users only gain access to data when they have the appropriate credentials. The benefits of IAM is not only related to deterrence of attacks. IAM also improves user experience, boost efficiency, increase flexibility, and lowers operating costs.

What are the steps to take to ensure business resilience?

- The first step should be enforcing basic password controls by requiring regular password resets and longer, complex passwords as well as hardening any system that allows employees or customers to reset passwords online.
- But password controls alone are not enough. Using multi-factor authentication combining something you know (password), with something you have (an RSA token) and/or something you are (like a thumbprint) makes it harder for bad actors to get into your network. It is also important to:
  - Harden the physical network environment in order to ensure assets are protected from interruption or data loss.
    - Limiting a user's access to only those that are necessary for completing the job.
    - Ensuring that users do not have more privileges than necessary.
      - For example, an IT system administrator may need "root" or "admin" access to complete some of their necessary tasks, but may improve security by logging in without those elevated privileges when they're not actively needed.
    - Logging and monitoring usage is a good practice, particularly with highly privileged (high risk) accounts to guard against misuse.

When it comes to sensitive data, it is critical for organizations to discover where data is located, protect the data, and control who has access to the data.