WEBINAR SUMMARY

August 20, 2024

INFORMATION WEEK

Tools & Technologies for Managing Cyber Risk in 2024

Candy Alexander, Chief Information Security Officer and Cyber Practice Lead, NeuEon, Inc.
Rex Booth, Chief Information Security Officer, SailPoint

Moderator
Brandon Taylor, Information Week

KEY TAKEAWAYS

- Increasingly distributed workforces and new technologies drive challenges in the 2024 risk landscape.
- Effective risk management in 2024 and beyond requires intentional, focused effort.
- Security leaders can achieve successful risk management through key best practices.
- Successful security transformation cannot happen without identity security.
- SailPoint leverages AI and machine learning to provide identity security for the cloud enterprise.

in partnership with

SailPoint

OVERVIEW

The digital landscape is constantly evolving. In today's interconnected world, powered by the cloud, AI, and remote work, a vast and complex risk landscape has emerged. Malicious threat actors continue to leverage tactics such as phishing, malware, social engineering, and even technology advances, but it is no longer about protecting the perimeter. That's because today there is no perimeter. With remote workforces requiring never-ending access, authentication and identity security are paramount.

SailPoint enables organizations to manage and govern access for every internal and external digital identity it serves. With SailPoint, organizations can improve IT efficiencies and reduce operational costs by shifting security from reactive to proactive, creating a secure technology ecosystem that fuels business transformation.

CONTEXT

Candy Alexander discussed the challenges of today's risk landscape. Rex Booth explained how identity security can help organizations address those challenges.

KEY TAKEAWAYS

Increasingly distributed workforces and new technologies drive challenges in the 2024 risk landscape.

In the past few years, the number of employees and organizations that have shifted to a remote workforce has grown exponentially. Remote workforces depend on accessing the enterprise environment from any location and any time zone, leading companies to increasingly adopt cloud and SaaS technologies to meet this requirement.

However, cloud-based solutions are often accompanied by the dual challenges of little to no visibility into, along with little to no control over, vendor environments and configurations as well as user access to those environments. Ensuring resiliency, controlling access to sensitive data and important applications, and ensuring standard operating procedures are constantly and consistently followed becomes significantly more challenging amid the proliferation of cloud and SaaS technologies.

> "When we don't know where our environments are or who controls it or how it's controlled, the risk is a huge question mark."
>
> *Candy Alexander, NeuEon*

The rise of AI is presenting additional security challenges, as more AI-powered solutions are implemented. Environments will only grow more complex, with the rapid growth and evolution of technologies that businesses rely on for global operations creating new weaknesses and vulnerabilities.

Figure 1: Realities of third-party risk

64%

third-party risk management is viewed as a **strategic imperative** by their board of directors and executive teams[1]

51%

have experienced a data breach caused by one of their third parties[2]

$4.29M

Average cost of a third-party breach[2]

63%

Don't have visibility into the access given to non-employees[2]

Effective risk management in 2024 and beyond requires intentional, focused effort.

To maintain security in this ever-changing risk landscape requires effective risk management. Risk management is the ability to determine potential harm and take appropriate steps to address it. But to successfully achieve this, gaining both visibility and control of actions over the environment is paramount.

In 2024 and 2025, risk management is centered on data: where it lives, who has access to it, what its purpose and value are, and more. Today, defining and adhering to a data governance strategy or policy is critical to risk management. Understanding the data lifecycle requires building a map of the data flow, including how the data enters the organization, which applications or end users receive the data and where is it transferred or stored, as well as which systems are used. Mapping the data flow will help to uncover where risks are and to ensure that the appropriate safeguards are put in place to protect the data as it moves through the environment.

> "Data is our new currency. [But] not all data is equal—nor is the technology that houses it."
>
> *Candy Alexander, NeuEon*

Looking beyond 2024, however, security leaders must begin shifting risk management from a reactive approach to a more proactive strategy.

For the past three decades, cybersecurity has been primarily a reactive endeavor. Threat actors have been the "leaders" who have shaped the field, while security teams play catch-up in responding to attacks. However, there is a growing desire among security practitioners to turn the paradigm on its head and relegate threat actors to a lesser role, with the goal of fostering a connected society that can harness the digital world as a force for good, without the level of risk present in today's landscape. But the shift from reactive to proactive does not happen without intentional, long-term effort. Transformation has to take place across three dimensions: vertical, horizontal, and temporal.

Figure 2: Three dimensions of transformation

Vertical

Improved connectivity and reduced dissonance within organizations and collaborative units

Horizontal

More equitable distribution of responsibility and risk across society

Temporal

Pursue a collective defense through early intervention and intercept precursors of malice earlier

Security leaders can achieve successful risk management through key best practices.

CISOs and other security leaders own the work of identifying risks and making recommendations for improvement in both the short and long term, as well as finding ways to continuously enable workers to use transformational technology in a safe way.

Best practices of an effective security leader include:

- Understand the risk profile of the company against the larger risk landscape and explain how security and risk mitigation efforts align with the business. Connecting risk with its impact on the business will help achieve the optimal balance between cost of risk and cost of operations and make transformative efforts more successful.
- Governance is key. Developing a security strategy that is reviewed and revised regularly must be a conscious, intentional effort within a larger organizational push. To help with strategy development, security leaders can make use of risk frameworks, which provide guidance for identifying, assessing, and managing risk. Examples of risk frameworks include the NIST Risk Management Framework (RMF) and recommendations from the Cloud Security Alliance.
- Installing or elevating a Chief Data Officer or equivalent role, who provides data oversight and data governance, can help maintain ongoing data security, as data owners and data consumers will change over time.
- Once an organization's risks are clearly identified and understood, bringing in AI-based technologies can greatly improve monitoring and mitigation. Solutions such as XDR, MDR, and EDR are strongly recommended as a baseline.

Successful security transformation cannot happen without identity security.

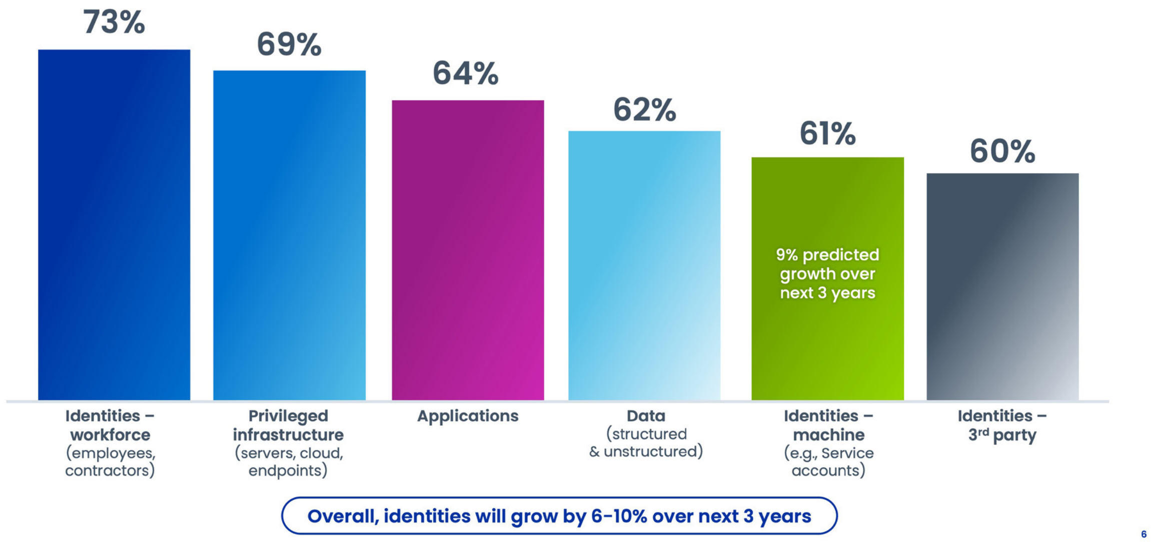
Identity security is essential to achieving both effective and proactive risk management, and forms a central pillar of a strong risk management strategy—in 2024 and beyond. Securely enabling users to access what they need, when they need it, is impossible without identity security.

> "Cybersecurity, in the positive sense, is about enabling the right people with the right access at the right time."
>
> *Rex Booth, SailPoint*

Over the past decades, different types of identity categories have emerged and grown. Identity of human users, such as employees and contractors, have the highest maturity in terms of security coverage. However, non-human user categories lag behind. In many organizations, the population of machine or non-human identities can outstrip human identities by orders of magnitude.

The rise of cloud and SaaS adoption require ever-greater attention to non-human identity access management; however, the numbers reveal that across industries, visibility into the access being given to these identity categories is lacking.

Figure 3: The state of maturity across identity categories



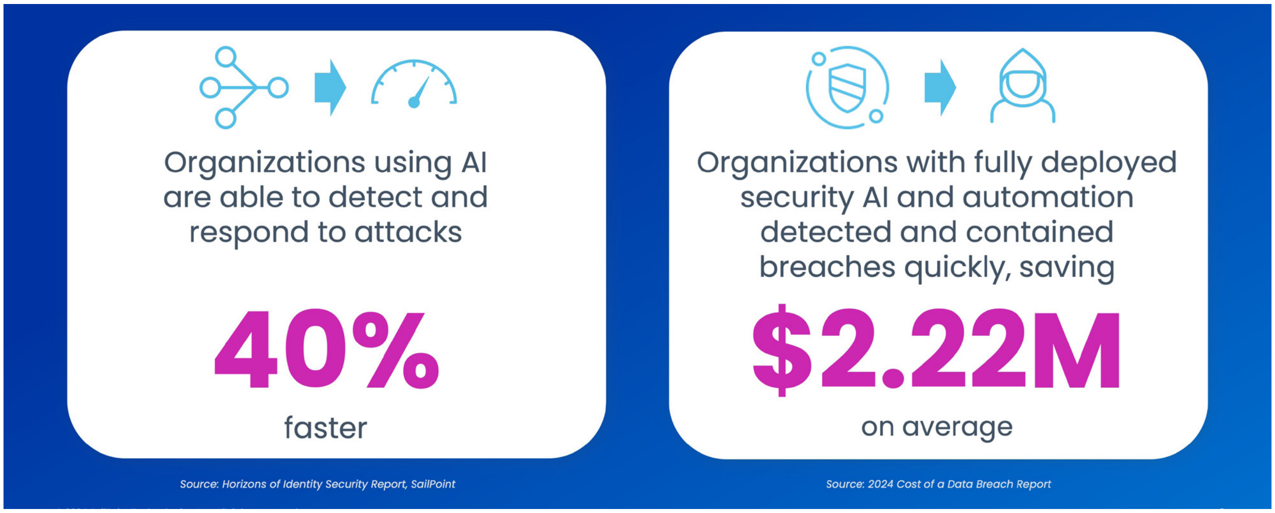
SailPoint leverages AI and machine learning to provide identity security for the cloud enterprise.

The need to increase identity coverage is a known problem that is not quite being solved by a good majority of organizations, for which there is increasing urgency. Because the number of identities, in general, is already well beyond human management, increasing identity coverage across all categories requires tools and capabilities that can leverage AI, machine learning, and automation to secure the environment and enable a security transformation.

The SailPoint unified identity security solution provides a singular, comprehensive data model driven by a robust policy engine that manages and protects all enterprise identities and their access across an organization. This unified approach brings significant clarity across who is doing what and when across the organization, enabling efficient—and highly secure—business operations. Using AI and ML technology, SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data, removing pockets of hidden risk.

As a category leader, SailPoint continuously reinvents identity security as the foundation of the secure enterprise, delivering a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency.

Figure 4: How AI-enabled technologies strengthen risk management



Organizations using AI are able to detect and respond to attacks

40%

faster

Source: Horizons of Identity Security Report, SailPoint

Organizations with fully deployed security AI and automation detected and contained breaches quickly, saving

$2.22M

on average

Source: 2024 Cost of a Data Breach Report

ADDITIONAL INFORMATION

To learn more, visit sailpoint.com.

BIOGRAPHIES

Candy Alexander

Chief Information Security Officer and Cyber Practice Lead, NeuEon, Inc.

Ms. Alexander is an international award-winning cybersecurity executive with over 30 years of experience. She is the CISO at NeuEon and the Cyber practice lead, assisting companies in improving their cyber risk & security programs through business alignment.

Ms. Alexander's contributions to the community include public speaking, with the most memorable being invited to speak at the United Nations and the Office of the Whitehouse. The media often interview her on many topics regarding cybersecurity and the cybersecurity profession. She is the immediate past International President of the ISSA, an international professional association for which she served two terms. She was the chief architect for the ISSA's Cyber Security Career Lifecycle. She is also the inaugural President and past Board Member of the ISSA Education and Research Foundation. Ms. Alexander has been instrumental in establishing the annual ISSA/ESG research project to understand better the challenges cybersecurity professionals worldwide face.

Rex Booth

Chief Information Security Officer, SailPoint

Rex Booth is the Chief Information Security Officer at SailPoint. In this role, he leads the full spectrum of cybersecurity strategy and operations at SailPoint, including enterprise operational security and product security. Rex came to SailPoint from the White House where he served as a Senior Policy Advisor and the Director of Stakeholder Engagement in the Office of the National Cyber Director. While there, he developed and executed strategies for national-level engagement with private sector and international stakeholders to pursue a more secure and resilient cyberspace. For over two decades, Rex has focused on the full spectrum of cybersecurity – from secure web development and architecting one of the first in-house SIEMs, to federal enterprise risk management, to incident response against state actors, national and international cyber collaboration and coordination, and operational leadership.

Brandon Taylor

Information Week (Moderator)

Brandon Taylor is the Digital Editorial Program Manager across Enterprise IT media brands: InformationWeek, Data Center Knowledge, ITPro Today, and Network Computing. He enables the successful delivery of sponsored content programs, secures speakers for the brands' many events, and assists in content strategy.

© 2024 Informa. All rights reserved.