




How Modern CISOs are putting security at the epicenter of innovation

June 2024





The role of the Chief Information Security Officer (CISO) is evolving rapidly in the digital era.

- How can CISOs keep up with the changing demands and expectations of their stakeholders, customers, and regulators?
- How can they leverage data and technology to enhance their security posture and business value?
- How can they align their strategy with the broader organizational goals and vision?

Table of contents

Chapter 1 pg. 03

Empower cyber defense and create resiliency with GenAI's capabilities

Chapter 2 pg. 05

Designing a resilient infrastructure that balances risk and agility

Chapter 3 pg. 08

Bolster digital trust with key investments in automation and infrastructure

Chapter 4 pg. 10

Building the new cyber operating model: Prioritizing people, process, and technology

Chapter 5 pg. 13

Understand the cost of breaches and attacks and how mature cybersecurity organizations can recover and maintain trust

Chapter 6 pg. 15

Overcome challenges by building modern, agile cybersecurity frameworks



Chapter 1

Empower cyber defense and create resiliency with GenAI's capabilities

Key findings

Seven in 10 senior executives (69%) say their organization will use generative AI (GenAI) for cyber defense in the next 12 months, according to the [2024 Global Digital Trust Insights](#) survey.

52% CISOs and CIOs should pay attention to a prevailing sentiment: 52% expect GenAI to lead to catastrophic cyber attacks in the next 12 months.

21% are already seeing benefits to their cyber programs because of GenAI.

37% About a third of this year's respondents agree that four types of regulation will be most important to securing the future growth of their organisation — regulation of AI.

Source: PwC's 2024 Global Digital Trust Insights Survey

GenAI presents a significant opportunity in the evolution of cyber defense, particularly in the areas of threat detection and analysis, as well as cyber risk and incident reporting.

Traditional signature-based detection systems often struggle to identify complex patterns and indicators of compromise. In contrast, GenAI excels at proactively detecting vulnerability exploits, synthesizing data, and providing actionable defense options. It simplifies incident response reporting, risk assessments, and regulatory compliance through natural language processing (NLP), which transforms technical data into concise content. For example, GenAI's NLP capabilities can translate technical data into understandable content for incident response reporting, threat intelligence, risk assessments, audits, and regulatory compliance. This is particularly valuable in the era of heightened cyber transparency, where timely and consistent reporting of cyber incidents is required by laws and regulations. GenAI goes beyond just reporting by providing easy-to-understand recommendations and even creating templates for industry standards and leading practices, streamlining the preparation of these reports.



Securing the cloud and software supply chain requires constant updates in security policies and controls. GenAI, powered by machine learning algorithms, can recommend, assess, and draft tailored security policies based on an organization's threat profile, technologies, and business objectives. This adaptive approach can help organizations respond to evolving threats and maintain a secure posture. For example, GenAI's adaptive controls can automate the assessment of risk scores for endpoints, as well as the review of access requests and permissions within a zero trust environment.

However, it is important to note that organizations implementing GenAI may face challenges such as the need for extensive data collection and analysis and concerns about ethical implications and biases. To address these challenges, responsible governance is crucial. Clear guidelines and policies should be established for data collection, storage, and usage, with regular updates to stay compliant with regulations. Training and education should be provided to confirm employees understand GenAI's capabilities and limitations, using it effectively and ethically. By approaching GenAI implementation responsibly, organizations can mitigate risks and increase its benefits in cybersecurity efforts.

Overall, GenAI's capabilities in threat detection, cyber risk and incident reporting, and adaptive controls offer significant advantages in the field of cyber defense. By leveraging GenAI's strengths, organizations can enhance their ability to detect and respond to threats, simplify reporting processes, and secure their cloud and software supply chain. To benefit from GenAI, organizations should carefully assess their specific needs and potential challenges, and confirm proper implementation and integration into their existing cybersecurity infrastructure.

How PwC is Innovating:

As GenAI technology continues to advance, its applications in cyber defense within AWS are expanding. PwC has developed fusion centers on top of Amazon Security Lake, utilizing the latest AWS AI technology, including Q and Bedrock. These technologies offer significant potential to enhance cybersecurity use cases by improving incident response and alerting capabilities, as well as enabling dynamic metrics reporting. For example, Bedrock provides actionable insights and can automate incident handling, enabling organizations to respond effectively to threats. Additionally, Q empowers CISOs to easily customize graphs and charts to suit their specific needs. By leveraging these technologies, organizations can strengthen their cybersecurity posture in the AWS environment and adapt to evolving threats.



Chapter 2

Designing a resilient infrastructure that balances risk and agility

Key findings

32%

Regulatory requirements for operational resilience.

Top 5% performers are 9x more likely to be mature in their cyber resilience practices.

Source: PwC's 2024 Global Digital Trust Insights Survey

Disruption is an inevitable part of the business landscape, as demonstrated by recent global events like the COVID-19 pandemic. In response, modern CISOs are taking the lead in building resilience plans to safeguard organizations from unforeseen challenges. While there is never a “silver bullet” there is one key area modern CISOs are investing time, money and energy into: Resilience.





Organizations should prioritize **four focus areas** to help enhance resilience:

1 Technology and Operational Resilience:

This pillar focuses on implementing measures to prevent and mitigate technical glitches, establishing the continuous functionality of critical systems, and having robust backup plans in place to address disruptions. Traditionally, organizations have referred to this pillar when discussing “disaster recovery” and “business continuity.” Examples of measures taken under this pillar may include redundant hardware and data centers, regular system backups, and thorough incident response plans.

2 Workforce Resilience:

This pillar emphasizes the importance of equipping the workforce with the skills, knowledge, and resources necessary for organizational resilience. It involves providing holistic training programs, establishing clear and effective communication channels, and fostering a culture that values and promotes resilience. By investing in employee development, organizations can confirm that their workforce is well-prepared to respond to and recover from disruptions. Examples of initiatives under this pillar may include conducting regular training sessions on incident response protocols, promoting cross-functional collaboration, and implementing employee assistance programs to support well-being during challenging times.

3 Data Resilience:

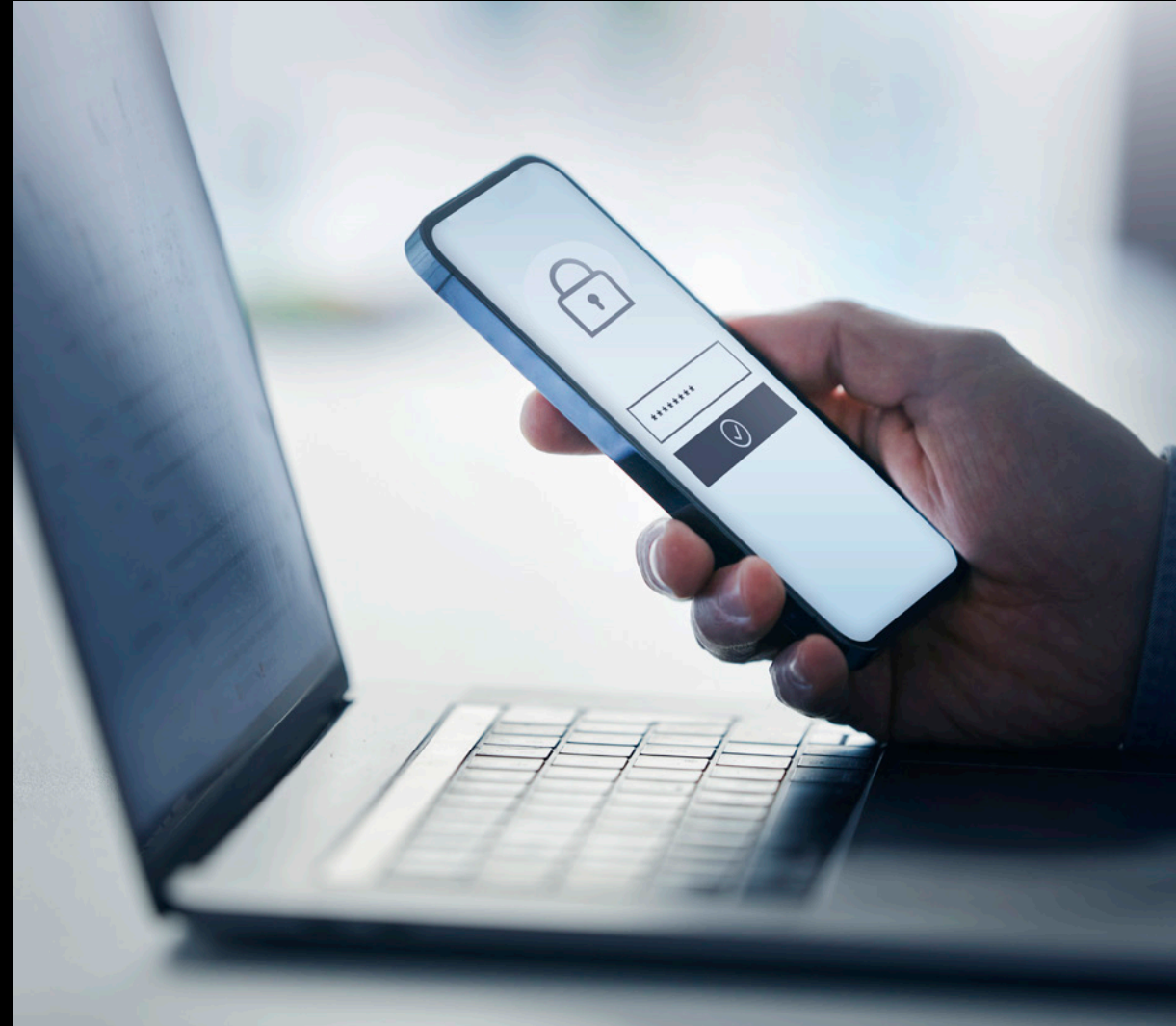
This pillar recognizes the value of data as a critical asset that requires protection and resilience against potential threats. It highlights the importance of implementing robust cybersecurity measures, backup and recovery strategies, and effective data governance practices to help establish the integrity and availability of data during disruptions. Organizations should treat data as a precious resource and take proactive steps to safeguard it. This may include implementing encryption and access controls, conducting regular data backups, and establishing data recovery plans. Additionally, organizations should adhere to data governance frameworks to maintain compliance with relevant regulations and industry leading practices. By prioritizing data resilience, organizations can mitigate the impacts of disruptions and maintain trust in their data assets.

4 Financial Resilience:

This pillar emphasizes the significance of maintaining a healthy budget to navigate through any challenges. It highlights the importance of financial resilience, including the establishment of contingency funds, conducting thorough financial risk assessments, and implementing effective financial planning strategies to mitigate the impacts of disruptions on the organization’s financial stability. By proactively managing finances, organizations can better handle unexpected events and maintain their financial health. Examples of initiatives under this pillar may include creating an emergency fund to address unforeseen expenses, regularly evaluating financial risks and developing mitigation plans, and implementing cost optimization measures to enable efficient resource allocation. By prioritizing financial resilience, organizations can enhance their ability to withstand disruptions and sustain their operations.



In collaboration with AWS, PwC offers support for organizations to help achieve all four types of resilience. AWS's advanced cloud infrastructure and services enhance technology and operational resilience, while PwC's expertise in workforce development and communication strategies strengthens workforce resilience. With AWS's security features and PwC's guidance, organizations can achieve data resilience. Furthermore, AWS's scalability and cost optimization, combined with PwC's financial planning strategies, facilitate financial resilience. By focusing on these four pillars, organizations can help bolster their ability to withstand and recover from disruptions, accelerating business continuity and mitigating the impacts of unforeseen events. This dance of resilience enables organizations to remain agile while effectively managing risk. In today's constantly disrupted business landscape, preparedness and swift response are crucial. By incorporating lessons learned and leveraging the expertise of modern CISOs, businesses can strengthen their resilience and successfully navigate the challenges ahead. PwC, in collaboration with AWS, is dedicated to accelerating these outcomes, providing organizations with the necessary tools and insights to not only survive but thrive in the face of disruption.





Chapter 3

Bolster digital trust with key investments in automation and infrastructure

Key findings

Invest more into cyber budget, with **85% increasing their cyber budget in 2024** (vs 79% overall), of which 19% are increasing cyber budget in 2024 by 15% or more, compared to 10% overall.

49% of cyber budgets aim to modernize technology including cyber infrastructure.

54% of these respondents cite cloud as their most pressing cybersecurity risk.

Investing in cybersecurity is paramount in today's digital era, as it enables organizations to enhance their financial resilience and effectively mitigate cyber risks. To achieve this, organizations should prioritize several critical areas to help bolster their digital trust and safeguard against cyber threats.

Source: PwC's 2024 Global Digital Trust Insights Survey





1 Threat intelligence and monitoring:

With the increasing sophistication of cyber attacks, organizations should stay vigilant and proactively identify potential risks. Investing in advanced threat intelligence tools and platforms enables real-time insights into emerging threats, empowering organizations to implement proactive defense strategies.

2 Identity and access management:

As businesses rely more on cloud infrastructure and remote working, confirming secure access to digital assets becomes crucial. Investing in robust identity and access management systems helps organizations establish strong authentication protocols, enforce access controls, and mitigate the risk of unauthorized access.

3 Security automation and orchestration:

The growing volume of security incidents requires organizations to automate security processes to effectively respond to threats. By investing in automation technologies, organizations can streamline security operations, reduce response times, and decrease human error.

4 Data protection and privacy:

Organizations should safeguard sensitive information, safeguard against data breaches, and comply with privacy regulations. Investing in encryption technologies, data loss prevention solutions, and robust data governance frameworks confirms data is secure and privacy is upheld.

The collaboration between AWS and PwC is highly relevant to these critical investment areas. AWS, as a leading cloud service provider, offers a wide range of security services to address these needs. They provide advanced threat intelligence capabilities, robust identity and access management tools, and security automation services. Additionally, AWS prioritizes data protection and privacy, offering encryption services and compliance frameworks.

By leveraging PwC 's cybersecurity consulting and risk management experience, the collaboration between AWS and PwC enhances organizations' ability to address these investment areas effectively. Together, they offer solutions that enable organizations to navigate the complex cybersecurity landscape, enhance their digital trust, and safeguard against evolving cyber threats.

In today's landscape, modern CISOs should align their priorities with Chief Financial Officers (CFOs) to prioritize these critical investment areas in cybersecurity. Collaboratively, CISOs and CFOs can establish the allocation of necessary resources and budget to invest in threat intelligence and monitoring, identity and access management, security automation and orchestration, and data protection and privacy. This alignment between CISOs and CFOs empowers organizations to fortify their digital trust, effectively combat cyber threats, and navigate the ever-changing cybersecurity landscape with confidence.



Chapter 4

Building the new cyber operating model: Prioritizing people, process, and technology

Key findings

Only half are 'very satisfied' with their technology capabilities in key cybersecurity areas.

40%

Ongoing security training as a key investment priority.

48%

Developing a new model for DevSecOps to better integrate security and technology development.

Source: PwC's 2024 Global Digital Trust Insights Survey

Modern CISOs should balance a cyber operating model built of people, process, and technology. By prioritizing the growth and development of their cybersecurity teams, implementing agile processes with specific strategies tailored to their organization's needs, and leveraging advanced technologies such as artificial intelligence (AI), machine learning (ML), and automation, CISOs can help enhance their organization's cyber posture and mitigate potential risks.





1 People: Addressing Technology Skill Gaps

The foundation of any successful cyber operating model lies in the people who drive it. CISOs should recognize the importance of building and growing their cybersecurity teams. This involves identifying and addressing technology skill gaps within the organization. CISOs should invest in training and development programs, such as hands-on workshops and certifications, to equip their teams with the necessary skills to effectively combat emerging cyber threats. Additionally, fostering a culture of continuous learning and knowledge sharing, through activities like regular team discussions and cross-training, can help create a skilled and resilient workforce. The collaboration between AWS and PwC provides opportunities for security teams to access specialized training programs and resources, leveraging the experience and industry insights from both organizations.

2 Process: Creating Cloud Native Agile Processes

To keep pace with the rapidly changing cyber landscape, organizations should adopt agile processes that enable quick and effective responses to threats. CISOs should focus on creating processes that promote flexibility and scalability, particularly in cloud-native environments. This could involve implementing DevSecOps practices, integrating security checks into each stage of the software development lifecycle, and utilizing automated security testing tools. By incorporating security into the early stages of the development lifecycle, organizations can help decrease vulnerabilities and reduce the risk of cyber attacks. The partnership between AWS and PwC offers opportunities for organizations to leverage the cloud-native capabilities of AWS and the cybersecurity experience of PwC to design and implement agile processes that align with their specific business requirements.

3 Technology: Enabling the Organization's Cyber Posture

While people and processes are crucial for maintaining a strong cyber posture, technology also plays a vital role. CISOs should leverage advanced technologies such as AI, ML, and automation to enhance their cybersecurity capabilities. For instance, AI-powered threat intelligence platforms can detect and respond to threats in real-time, ML algorithms can identify anomalous patterns indicative of cyber attacks, and automation tools can streamline routine security tasks. To further enhance their security posture, organizations can benefit from partnering with industry leaders like PwC and AWS. Through their collaborative efforts, fusion center implementations have been developed, offering dedicated cybersecurity capabilities within organizations' environments. These fusion centers, provide access to specialized knowledge and resources, enabling the activation of key AI, ML, and NLP capabilities to improve log analysis and strengthen security measures. This collaborative approach confirms that organizations can effectively respond to evolving cyber threats and increase the potential of advanced technologies.



To address cyber threats effectively, modern CISOs should prioritize people, process, and technology. By investing in their cybersecurity teams, addressing skill gaps, and fostering a culture of continuous learning, CISOs can build a skilled and resilient workforce. Implementing agile processes, especially in cloud-native environments, enables flexibility and scalability to respond to evolving threats. Leveraging advanced technologies like AI, ML, and automation enhances cybersecurity capabilities, from real-time threat detection to streamlined security tasks. Collaborating with industry leaders such as PwC and AWS offers access to specialized expertise and resources, such as fusion center implementations that can improve log analysis and strengthen security measures. This approach equips organizations to enhance their cyber posture and effectively mitigate risks in the ever-changing digital landscape.





Chapter 5

Understand the cost of breaches and attacks and how mature cybersecurity organizations can recover and maintain trust

The cost of security breaches continues to rise, with businesses experiencing significant financial losses and reputational damage. According to PwC's [2024 Global Digital Trust Insights](#) survey, the proportion of businesses reporting data breaches of over \$1 million has increased from 27% to 36% year over year. In response to this alarming trend, organizations are investing in cybersecurity initiatives and turning to advanced solutions like fusion center built on Amazon Security Lake.

1 The Growing Impact of Data Breaches

PwC's survey of 3,800 business and tech leaders across 71 countries reveals a concerning increase in data breaches. The healthcare industry, in particular, has been heavily impacted, with a global average cost of \$4.4 million for a damaging cyber- attack. In the healthcare sector, this cost rises by 25% to \$5.3 million. Alarming, 47% of healthcare organizations reported data breaches exceeding \$1 million. These statistics emphasize the urgent need for robust cybersecurity measures.

2 The Maturity of Cybersecurity Initiatives

Organizations that demonstrate greater maturity in their cybersecurity initiatives report a lower incidence of costly breaches. PwC's survey highlights the correlation between cybersecurity maturity and the number of benefits experienced. By investing in cybersecurity strategies, organizations can mitigate risks and safeguard their valuable assets. This includes leveraging advanced solutions like fusion centers implemented by PwC in AWS.

3 PwC Implementations of Fusion Centers Leveraging Amazon Security Lake

To address the evolving cyber threat landscape, PwC has developed a modernized fusion center, combining PwC's industry experience with the power of Amazon Security Lake, enabling organizations to detect and respond to threats effectively. The integration with Amazon Security Lake allows for centralized data storage and analysis, leveraging advanced analytics, machine learning, and artificial intelligence. This can empower CISOs to make data-driven decisions and strengthen their defenses.



Fusion centers offer numerous benefits for organizations seeking to enhance their cybersecurity posture. Real-time threat intelligence and proactive monitoring enable swift incident response, minimizing the impact of breaches. The fusion center's advanced analytics and GenAI capabilities help prioritize security investments effectively. Additionally, the integration with Amazon Security Lake enables scalability, flexibility, and cost-efficiency in managing and analyzing security data.

The rising cost of security breaches underscores the critical importance of investing in robust cybersecurity measures. PwC's [**2024 Global Digital Trust Insights**](#) survey reveals an alarming increase in data breaches, particularly in the healthcare industry. To address these threats effectively, organizations should prioritize cybersecurity maturity and leverage advanced solutions like the fusion center built on Amazon Security Lake. By doing so, organizations can detect and respond to threats swiftly, safeguard their valuable assets, and mitigate the financial and reputational risks associated with cyberattacks. Investing in holistic cybersecurity strategies is essential for organizations to maintain trust, safeguard sensitive data, and thrive in today's digital landscape.





Chapter 6

Overcome challenges by building modern, agile cybersecurity frameworks

CISOs face numerous challenges in building modern, agile cybersecurity practices. As organizations grow and adapt to new technologies, CISOs should establish an operating model that can scale and flex to address the importance of agility and scalability in safeguarding organizations from emerging threats.

1 Evolving Threat Landscape

One of the primary challenges for CISOs is the ever-evolving threat landscape. Cybercriminals constantly develop new techniques and exploit vulnerabilities in emerging technologies. CISOs should stay ahead of these threats by continuously updating their knowledge and skills, as well as implementing proactive security measures. This requires an agile approach that can adapt to new threats and vulnerabilities as they emerge.

2 Balancing Business Growth and Vulnerabilities

As organizations grow and adopt new technologies, their attack surface expands, making them more vulnerable to cyber threats. CISOs should strike a balance between supporting business growth and mitigating potential risks. This involves establishing scalable cybersecurity practices that can flex to accommodate the changing needs of the organization. By aligning Security measures with business objectives, CISOs can confirm that cybersecurity remains an integral part of the organization's growth strategy.

3 Establishing a Culture of Security

Building a modern cybersecurity operating model requires establishing a culture of security throughout the organization. CISOs should educate employees about the importance of cybersecurity and foster a sense of responsibility among all staff members. This includes implementing robust training programs, conducting regular security awareness campaigns, and encouraging a proactive approach to identifying and reporting potential threats. By involving all employees in the cybersecurity efforts, CISOs can help create a strong defense against cyberattacks.

4 Embracing Agile Methodologies

To address the challenges of scalability and flexibility, CISOs should embrace agile methodologies in their cybersecurity practices. Agile methodologies, such as DevSecOps, enable organizations to integrate security into the development and deployment processes. This confirms that security measures are implemented from the outset, reducing vulnerabilities and minimizing the need for retroactive fixes. By adopting an agile approach, CISOs can respond quickly to emerging threats and adapt their security practices accordingly.

5 Leveraging Technology and Automation

Modern cybersecurity practices heavily rely on technology and automation. CISOs should leverage advanced technologies, such as artificial intelligence, machine learning, and automation, to enhance their cybersecurity capabilities. These technologies can help detect and respond to threats in real-time, automate routine security tasks, and provide valuable insights for proactive decision-making. By embracing technology, CISOs can improve the efficiency and effectiveness of their cybersecurity operations.



Building modern, agile cybersecurity practices is a complex task for CISOs. By addressing the challenges of the evolving threat landscape, balancing business growth and vulnerabilities, establishing a culture of security, embracing agile methodologies, and leveraging technology and automation, CISOs can develop a robust cybersecurity operating model. This model can enable organizations to scale and flex their security practices to help address vulnerabilities effectively. By prioritizing agility and scalability, CISOs can help safeguard their organizations from emerging threats and confirm that cybersecurity remains a top priority in today's dynamic digital landscape.





PwC and AWS can help your organization tap into the power of fusion centers, which allow you to combine data from a variety of sources to create a centralized, near real-time view.

[Learn more](#)

[Click here](#) if you'd like to learn more about how PwC and AWS can help your organization tap into the power of fusion centers.